National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 - 15 Sep 2020 Vol. 07 No. 17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
163					
netease_youdao_dictionary					
Untrusted Search Path	03-Sep-20	4.4	NetEase Youdao Dictionary has a DLL hijacking vulnerability, which can be exploited by attackers to gain server permissions. This affects Guangzhou NetEase Youdao Dictionary 8.9.2.0. **CVE ID : CVE-2020-24159**	N/A	A-163-NETE-180920/1
netease_mail_master					
Untrusted Search Path	03-Sep-20	4.4	Guangzhou NetEase Mail Master 4.14.1.1004 on Windows has a DLL hijacking vulnerability. Attackers can use this vulnerability to execute malicious code. **CVE ID : CVE-2020-24161**	N/A	A-163-NETE-180920/2
360					
speed_browser					
Untrusted Search Path	03-Sep-20	4.4	360 Speed Browser 12.0.1247.0 has a DLL hijacking vulnerability, which can be exploited by attackers to execute malicious code. It is a dual-core browser owned by Beijing Qihoo Technology. **CVE ID : CVE-2020-24158**	N/A	A-360-SPEE-180920/3
Accusoft					
imagegear					

CVSS Scoring Scale	0-1	1-2	2-3	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	01-Sep-20	7.5	A memory corruption vulnerability exists in the TIFF handle_COMPRESSION_PACKBITS functionality of Accusoft ImageGear 19.7. A specially crafted malformed file can cause a memory corruption. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2020-6151**	N/A	A-ACC-IMAG-180920/4
Out-of-bounds Write	01-Sep-20	6.8	A code execution vulnerability exists in the DICOM parse_dicom_meta_info functionality of Accusoft ImageGear 19.7. A specially crafted malformed file can cause an out-of-bounds write. An attacker can trigger this vulnerability by providing a victim with a malicious DICOM file. **CVE ID : CVE-2020-6152**	N/A	A-ACC-IMAG-180920/5
Adobe					
experience_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	6	The AEM Forms add-on for versions 6.5.5.0 (and below) and 6.4.8.2 (and below) are affected by a stored XSS vulnerability that allows users with 'Author' privileges to store malicious scripts in fields associated with the Sites component. These scripts may be executed in a victim's browser when they open the page containing the vulnerable field.	N/A	A-ADO-EXPE-180920/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9732		
Information Exposure	10-Sep-20	5	An AEM java servlet in AEM versions 6.5.5.0 (and below) and 6.4.8.1 (and below) executes with the permissions of a high privileged service user. If exploited, this could lead to read-only access to sensitive data in an AEM repository. **CVE ID : CVE-2020-9733**	N/A	A-ADO-EXPE-180920/7
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	The AEM Forms add-on for versions 6.5.5.0 (and below) and 6.4.8.1 (and below) is affected by a stored XSS vulnerability that allows users with 'Author' privileges to store malicious scripts in fields associated with the Forms component. These scripts may be executed in a victim's browser when they open the page containing the vulnerable field. **CVE ID : CVE-2020-9734**	N/A	A-ADO-EXPE-180920/8
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by a stored XSS vulnerability that allows users with access to the Content Repository Development Environment to store malicious scripts in certain node fields. These scripts may be executed in a victim's browser when search queries return the page containing the	N/A	A-ADO-EXPE-180920/9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerable field. **CVE ID : CVE-2020-9735**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by a stored XSS vulnerability that allows users with access to the Content Repository Development Environment to store malicious scripts in certain node fields. These scripts may be executed in a victim's browser when browsing to the page containing the vulnerable field. **CVE ID : CVE-2020-9736**	N/A	A-ADO-EXPE-180920/10
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	4.3	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by a stored XSS vulnerability that allows users with access to the Content Repository Development Environment to store malicious scripts in certain node fields. These scripts may be executed in a victim's browser when they open the page containing the vulnerable field. **CVE ID : CVE-2020-9737**	N/A	A-ADO-EXPE-180920/11
Improper Neutralization of Input During Web Page	10-Sep-20	3.5	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by a stored XSS	N/A	A-ADO-EXPE-180920/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			vulnerability that allows users with access to the Content Repository Development Environment to store malicious scripts in certain node fields. These scripts may be executed in a victim's browser when visiting the page containing the vulnerable field. **CVE ID : CVE-2020-9738**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by a stored XSS vulnerability that allows users with 'Author' privileges to store malicious scripts in fields associated with the Design Importer. These scripts may be executed in a victim's browser when they open the page containing the vulnerable field. **CVE ID : CVE-2020-9740**	N/A	A-ADO-EXPE-180920/13
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	The AEM forms add-on for versions 6.5.5.0 (and below) and 6.4.8.2 (and below) is affected by a stored XSS vulnerability that allows users with 'Author' privileges to store malicious scripts in fields associated with the Forms component. These scripts may be executed in a victim's browser when they open the page containing the vulnerable field.	N/A	A-ADO-EXPE-180920/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9741		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-Sep-20	4.3	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by an HTML injection vulnerability in the content editor component that allows unauthenticated users to craft an HTTP request that includes arbitrary HTML code in a parameter value. An attacker could then use the malicious GET request to lure victims to perform unsafe actions in the page (ex. phishing). **CVE ID : CVE-2020-9743**	N/A	A-ADO-EXPE-180920/15
indesign					
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	6.8	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user. **CVE ID : CVE-2020-9727**	N/A	A-ADO-INDE-180920/16
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	6.8	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the	N/A	A-ADO-INDE-180920/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			current user. **CVE ID : CVE-2020-9728**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	6.8	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user. **CVE ID : CVE-2020-9729**	N/A	A-ADO-INDE-180920/18
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	6.8	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user. **CVE ID : CVE-2020-9730**	N/A	A-ADO-INDE-180920/19
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	6.8	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user. **CVE ID : CVE-2020-9731**	N/A	A-ADO-INDE-180920/20
experience_manager_forms					
Improper Neutralizati	10-Sep-20	6	The AEM Forms add-on for versions 6.5.5.0 (and below)	N/A	A-ADO-EXPE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			and 6.4.8.2 (and below) are affected by a stored XSS vulnerability that allows users with 'Author' privileges to store malicious scripts in fields associated with the Sites component. These scripts may be executed in a victim's browser when they open the page containing the vulnerable field. **CVE ID : CVE-2020-9732**		180920/21
Information Exposure	10-Sep-20	5	An AEM java servlet in AEM versions 6.5.5.0 (and below) and 6.4.8.1 (and below) executes with the permissions of a high privileged service user. If exploited, this could lead to read-only access to sensitive data in an AEM repository. **CVE ID : CVE-2020-9733**	N/A	A-ADO-EXPE-180920/22
framemaker					
Out-of-bounds Write	10-Sep-20	6.8	Adobe FrameMaker version 2019.0.6 (and earlier versions) lacks proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. This could be exploited to execute arbitrary code with the privileges of the current user. User interaction is required to exploit this vulnerability in that the target must open a malicious FrameMaker file. **CVE ID : CVE-2020-9725**	N/A	A-ADO-FRAM-180920/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Sep-20	5.8	Adobe FrameMaker version 2019.0.6 (and earlier versions) has an out-of-bounds read vulnerability that could be exploited to read past the end of an allocated buffer, possibly resulting in a crash or disclosure of sensitive information from other memory locations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious FrameMaker file. **CVE ID : CVE-2020-9726**	N/A	A-ADO-FRAM-180920/24
advanced_reports_project					
advanced_reports					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	silverstripe-advancedreports (aka the Advanced Reports module for SilverStripe) 1.0 through 2.0 is vulnerable to Cross-Site Scripting (XSS) because it is possible to inject and store malicious JavaScript code. The affects admin/advanced-reports/DataObjectReport/EditForm/field/DataObjectReport/item (aka report preview) when an SVG document is provided in the Description parameter. **CVE ID : CVE-2020-25102**	N/A	A-ADV-ADVA-180920/25
Apache					
activemq					
Improper Authenticat	10-Sep-20	4.3	Apache ActiveMQ uses LocateRegistry.createRegistry	N/A	A-APA-ACTI-180920/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion			() to create the JMX RMI registry and binds the server to the "jmxrmi" entry. It is possible to connect to the registry without authentication and call the rebind method to rebind jmxrmi to something else. If an attacker creates another server to proxy the original, and bound that, he effectively becomes a man in the middle and is able to intercept the credentials when an user connects. Upgrade to Apache ActiveMQ 5.15.12. **CVE ID : CVE-2020-13920**		
netbeans					
N/A	09-Sep-20	7.5	To be able to analyze gradle projects, the build scripts need to be executed. Apache NetBeans follows this pattern. This causes the code of the build script to be invoked at load time of the project. Apache NetBeans up to and including 12.0 did not request consent from the user for the analysis of the project at load time. This in turn will run potentially malicious code, from an external source, without the consent of the user. **CVE ID : CVE-2020-11986**	N/A	A-APA-NETB-180920/27
cassandra					
Exposure of Resource to Wrong	01-Sep-20	4.3	In Apache Cassandra, all versions prior to 2.1.22, 2.2.18, 3.0.22, 3.11.8 and 4.0-	N/A	A-APA-CASS-180920/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			beta2, it is possible for a local attacker without access to the Apache Cassandra process or configuration files to manipulate the RMI registry to perform a man-in-the-middle attack and capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and perform unauthorised operations. Users should also be aware of CVE-2019-2684, a JRE vulnerability that enables this issue to be exploited remotely. **CVE ID : CVE-2020-13946**		
appsbd					
best_support_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-20	3.5	An Authenticated Persistent XSS vulnerability was discovered in the Best Support System, tested version v3.0.4. **CVE ID : CVE-2020-24963**	N/A	A-APP-BEST-180920/29
arr-flatten-unflatten_project					
arr-flatten-unflatten					
Improper Input Validation	01-Sep-20	7.5	All versions of package arr-flatten-unflatten are vulnerable to Prototype Pollution via the constructor. **CVE ID : CVE-2020-7713**	https://snyk.io/vuln/SNYK-JS-ARRFLATTENUNFLATTEN-598396	A-ARR-ARR--180920/30
Artifex					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ghostscript					
Use After Free	03-Sep-20	2.1	A use after free was found in igc_reloc_struct_ptr() of psi/igc.c of ghostscript-9.25. A local attacker could supply a specially crafted PDF file to cause a denial of service. **CVE ID : CVE-2020-14373**	N/A	A-ART-GHOS-180920/31
Arubanetworks					
analytics_and_location_engine					
N/A	04-Sep-20	4	A vulnerability exists in the Aruba Analytics and Location Engine (ALE) web management interface 2.1.0.2 and earlier firmware that allows an already authenticated administrative user to arbitrarily modify files as an underlying privileged operating system user. **CVE ID : CVE-2020-7119**	N/A	A-ARU-ANAL-180920/32
atftp_project					
atftp					
Reachable Assertion	10-Sep-20	5	An exploitable denial of service vulnerability exists in the atftpd daemon functionality of atftp 0.7.git20120829-3.1+b1. A specially crafted sequence of RRQ-Multicast requests trigger an assert() call resulting in denial-of-service. An attacker can send a sequence of malicious packets to trigger this vulnerability. **CVE ID : CVE-2020-6097**	N/A	A-ATF-ATFT-180920/33
Atlassian					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jira					
Information Exposure	01-Sep-20	5	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to enumerate project keys via an Information Disclosure vulnerability in the /browse.PROJECTKEY endpoint. The affected versions are before version 7.13.7, from version 8.0.0 before 8.5.8, and from version 8.6.0 before 8.12.0. **CVE ID : CVE-2020-14178**	N/A	A-ATL-JIRA-180920/34
jira_software_data_center					
Information Exposure	01-Sep-20	5	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to enumerate project keys via an Information Disclosure vulnerability in the /browse.PROJECTKEY endpoint. The affected versions are before version 7.13.7, from version 8.0.0 before 8.5.8, and from version 8.6.0 before 8.12.0. **CVE ID : CVE-2020-14178**	N/A	A-ATL-JIRA-180920/35
autoptimize					
autoptimize					
Unrestricted Upload of File with Dangerous Type	03-Sep-20	6.5	The ao_ccss_import AJAX call in Autoptimize Wordpress Plugin 2.7.6 does not ensure that the file provided is a legitimate Zip file, allowing high privilege users to upload arbitrary files, such as PHP, leading to remote command	N/A	A-AUT-AUTO-180920/36

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-24948**		
Avast					
antivirus					
Insufficiently Protected Credentials	10-Sep-20	2.1	An issue was discovered in the Login Password feature of the Password Manager component in Avast Antivirus 20.1.5069.562. An entered password continues to be stored in Windows main memory after a logout, and after a Lock Vault operation. **CVE ID : CVE-2020-15024**	N/A	A-AVA-ANTI-180920/37
Bitcoin					
bitcoin_core					
N/A	10-Sep-20	5	Bitcoin Core 0.20.0 allows remote denial of service. **CVE ID : CVE-2020-14198**	N/A	A-BIT-BITC-180920/38
Canonical					
ppp					
Information Exposure	01-Sep-20	2.1	The modprobe child process in the ./debian/patches/load_ppp_generic_if_needed patch file incorrectly handled module loading. A local non-root attacker could exploit the MODPROBE_OPTIONS environment variable to read arbitrary root files. Fixed in 2.4.5-5ubuntu1.4, 2.4.5-5.1ubuntu2.3+esm2, 2.4.7-1+2ubuntu1.16.04.3, 2.4.7-2+2ubuntu1.3, 2.4.7-2+4.1ubuntu5.1, 2.4.7-2+4.1ubuntu6. Was ZDI-CAN-	N/A	A-CAN-PPP-180920/39

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11504. **CVE ID : CVE-2020-15704**		
chadhaajay					
phpkb					
Improper Input Validation	03-Sep-20	5	An issue was discovered in Chadha PHPKB 9.0 Enterprise Edition. installer/test-connection.php (part of the installation process) allows a remote unauthenticated attacker to disclose local files on hosts running PHP before 7.2.16, or on hosts where the MySQL ALLOW LOCAL DATA INFILE option is enabled. **CVE ID : CVE-2020-11579**	N/A	A-CHA-PHPK-180920/40
Cisco					
enterprise_network_function_virtualization_infrastructure					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-20	4	A vulnerability in the directory permissions of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker to perform a directory traversal attack on a limited set of restricted directories. The vulnerability is due to a flaw in the logic that governs directory permissions. An attacker could exploit this vulnerability by using capabilities that are not controlled by the role-based access control (RBAC) mechanisms of the software. A successful exploit could allow the attacker to overwrite files on an affected device.	N/A	A-CIS-ENTE-180920/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3365		
Improper Input Validation	04-Sep-20	5.5	A vulnerability in the REST API of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker to overwrite certain files that should be restricted on an affected device. The vulnerability is due to insufficient authorization enforcement on an affected system. An attacker could exploit this vulnerability by uploading a file using the REST API. A successful exploit could allow an attacker to overwrite and upload files, which could degrade the functionality of the affected system. **CVE ID : CVE-2020-3478**	N/A	A-CIS-ENTE-180920/42
jabber					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Sep-20	9.3	A vulnerability in the application protocol handling features of Cisco Jabber for Windows could allow an unauthenticated, remote attacker to execute arbitrary commands. The vulnerability is due to improper handling of input to the application protocol handlers. An attacker could exploit this vulnerability by convincing a user to click a link within a message sent by email or other messaging platform. A successful exploit could allow the attacker to	N/A	A-CIS-JABB-180920/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands on a targeted system with the privileges of the user account that is running the Cisco Jabber client software. **CVE ID : CVE-2020-3430**		
Improper Input Validation	04-Sep-20	9	A vulnerability in Cisco Jabber for Windows could allow an authenticated, remote attacker to execute arbitrary code. The vulnerability is due to improper validation of message contents. An attacker could exploit this vulnerability by sending specially crafted Extensible Messaging and Presence Protocol (XMPP) messages to the affected software. A successful exploit could allow the attacker to cause the application to execute arbitrary programs on the targeted system with the privileges of the user account that is running the Cisco Jabber client software, possibly resulting in arbitrary code execution. **CVE ID : CVE-2020-3495**	N/A	A-CIS-JABB-180920/44
Improper Input Validation	04-Sep-20	4	A vulnerability in Cisco Jabber software could allow an authenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper validation of message contents. An attacker could exploit this vulnerability by sending specially crafted messages to a	N/A	A-CIS-JABB-180920/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			targeted system. A successful exploit could allow the attacker to cause the application to return sensitive authentication information to another system, possibly for use in further attacks. **CVE ID : CVE-2020-3498**		
Improper Input Validation	04-Sep-20	3.5	A vulnerability in Cisco Jabber for Windows software could allow an authenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper validation of message contents. An attacker could exploit this vulnerability by sending specially crafted messages that contain Universal Naming Convention (UNC) links to a targeted user and convincing the user to follow the provided link. A successful exploit could allow the attacker to cause the application to access a remote system, possibly allowing the attacker to gain access to sensitive information that the attacker could use in additional attacks. **CVE ID : CVE-2020-3537**	N/A	A-CIS-JABB-180920/46
webex_teams					
Information Exposure Through Log Files	04-Sep-20	2.1	A vulnerability in the media engine component of Cisco Webex Meetings Client for Windows, Cisco Webex Meetings Desktop App for Windows, and Cisco Webex	N/A	A-CIS-WEBE-180920/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Teams for Windows could allow an authenticated, local attacker to gain access to sensitive information. The vulnerability is due to unsafe logging of authentication requests by the affected software. An attacker could exploit this vulnerability by reading log files that are stored in the application directory. A successful exploit could allow the attacker to gain access to sensitive information, which could be used in further attacks. **CVE ID : CVE-2020-3541**		
webex_training					
Improper Input Validation	04-Sep-20	4	A vulnerability in Cisco Webex Training could allow an authenticated, remote attacker to join a password-protected meeting without providing the meeting password. The vulnerability is due to improper validation of input to API requests that are a part of meeting join flow. An attacker could exploit this vulnerability by sending an API request to the application, which would return a URL that includes a meeting join page that is prepopulated with the meeting username and password. A successful exploit could allow the attacker to join the password-protected meeting. The attacker would be visible in the attendee list	N/A	A-CIS-WEBE-180920/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the meeting. **CVE ID : CVE-2020-3542**		
webex_meetings					
Information Exposure Through Log Files	04-Sep-20	2.1	A vulnerability in the media engine component of Cisco Webex Meetings Client for Windows, Cisco Webex Meetings Desktop App for Windows, and Cisco Webex Teams for Windows could allow an authenticated, local attacker to gain access to sensitive information. The vulnerability is due to unsafe logging of authentication requests by the affected software. An attacker could exploit this vulnerability by reading log files that are stored in the application directory. A successful exploit could allow the attacker to gain access to sensitive information, which could be used in further attacks. **CVE ID : CVE-2020-3541**	N/A	A-CIS-WEBE-180920/49
cloudfoundry					
cf-deployment					
Incorrect Authorization	03-Sep-20	4	Cloud Foundry CAPI (Cloud Controller) versions prior to 1.98.0 allow authenticated users having only the "cloud_controller.read" scope, but no roles in any spaces, to list all droplets in all spaces (whereas they should see none). **CVE ID : CVE-2020-5418**	https://www.cloudfoundry.org/blog/cve-2020-5418	A-CLO-CF-D-180920/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	03-Sep-20	6.8	Cloud Foundry Routing (Gorouter) versions prior to 0.206.0 allow a malicious developer with "cf push" access to cause denial-of-service to the CF cluster by pushing an app that returns specially crafted HTTP responses that crash the Gorouters. **CVE ID : CVE-2020-5420**	https://www.cloudfoundry.org/blog/cve-2020-5420	A-CLO-CF-D-180920/51
capi-release					
Incorrect Authorization	03-Sep-20	4	Cloud Foundry CAPI (Cloud Controller) versions prior to 1.98.0 allow authenticated users having only the "cloud_controller.read" scope, but no roles in any spaces, to list all droplets in all spaces (whereas they should see none). **CVE ID : CVE-2020-5418**	https://www.cloudfoundry.org/blog/cve-2020-5418	A-CLO-CAPI-180920/52
gorouter					
Improper Check for Unusual or Exceptional Conditions	03-Sep-20	6.8	Cloud Foundry Routing (Gorouter) versions prior to 0.206.0 allow a malicious developer with "cf push" access to cause denial-of-service to the CF cluster by pushing an app that returns specially crafted HTTP responses that crash the Gorouters. **CVE ID : CVE-2020-5420**	https://www.cloudfoundry.org/blog/cve-2020-5420	A-CLO-GORO-180920/53
Concrete5					
concrete5					
Unrestricte	04-Sep-20	9	Concrete5 up to and including	N/A	A-CON-CONC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Upload of File with Dangerous Type			8.5.2 allows Unrestricted Upload of File with Dangerous Type such as a .php file via File Manager. It is possible to modify site configuration to upload the PHP file and execute arbitrary commands. **CVE ID : CVE-2020-24986**		180920/54
ctrip					
apollo					
Improper Input Validation	10-Sep-20	6.8	apollo-adminservice before version 1.7.1 does not implement access controls. If users expose apollo-adminservice to internet(which is not recommended), there are potential security issues since apollo-adminservice is designed to work in intranet and it doesn't have access control built-in. Malicious hackers may access apollo-adminservice apis directly to access/edit the application's configurations. To fix the potential issue without upgrading, simply follow the advice that do not expose apollo-adminservice to internet. **CVE ID : CVE-2020-15170**	https://github.com/ctripcorp/apollo/security/advisories/GHSA-xpmx-h7xq-xffh	A-CTR-APOL-180920/55
daily_tracker_system_project					
daily_tracker_system					
Improper Neutralization of Special	03-Sep-20	7.5	A SQL injection vulnerability in login in Sourcecodetester Daily Tracker System 1.0 allows unauthenticated user	N/A	A-DAI-DAIL-180920/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			to execute authentication bypass with SQL injection via the email parameter. **CVE ID : CVE-2020-24193**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-20	4.3	A Cross-site scripting (XSS) vulnerability in 'user-profile.php' in SourceCodester Daily Tracker System v1.0 allows remote attackers to inject arbitrary web script or HTML via the 'fullname' parameter. **CVE ID : CVE-2020-24194**	N/A	A-DAI-DAIL-180920/57
Debian					
freedombox					
Exposure of Resource to Wrong Sphere	02-Sep-20	5	FreedomBox through 20.13 allows remote attackers to obtain sensitive information from the /server-status page of the Apache HTTP Server, because a connection from the Tor onion service (or from PageKite) is considered a local connection. This affects both the freedombox and plinth packages of some Linux distributions, but only if the Apache mod_status module is enabled. **CVE ID : CVE-2020-25073**	N/A	A-DEB-FREE-180920/58
deep-get-set_project					
deep-get-set					
Improper Input Validation	01-Sep-20	7.5	All versions of package deep-get-set are vulnerable to Prototype Pollution via the	N/A	A-DEE-DEEP-180920/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			main function. **CVE ID : CVE-2020-7715**		
Dell					
emc_elastic_cloud_storage					
Exposure of Resource to Wrong Sphere	02-Sep-20	5	Dell EMC ECS, versions prior to 3.5, contains an Exposure of Resource vulnerability. A remote unauthenticated attacker can access the list of DT (Directory Table) objects of all internally running services and gain knowledge of sensitive data of the system. **CVE ID : CVE-2020-5386**	N/A	A-DEL-EMC_-180920/60
emc_isilon_onefs					
Incorrect Permission Assignment for Critical Resource	02-Sep-20	6.5	Dell EMC Isilon OneFS versions 8.2.2 and earlier and Dell EMC PowerScale OneFS version 9.0.0 contain a privilege escalation vulnerability. An authenticated malicious user may exploit this vulnerability by using SyncIQ to gain unauthorized access to system management files. **CVE ID : CVE-2020-5369**	N/A	A-DEL-EMC_-180920/61
derhansen					
event_management_and_registration					
Incorrect Authorization	02-Sep-20	4	The sf_event_mgt (aka Event management and registration) extension before 4.3.1 and 5.x before 5.1.1 for TYPO3 allows Information Disclosure (participant data, and event data via email) because of Broken Access Control.	https://typo3.org/security/advisory/typo3-ext-sa-2020-017	A-DER-EVEN-180920/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-25026		
digitalbazzar					
forge					
Improper Input Validation	01-Sep-20	7.5	The package node-forge before 0.10.0 is vulnerable to Prototype Pollution via the util.setPath function. Note: Version 0.10.0 is a breaking change removing the vulnerable functions. **CVE ID : CVE-2020-7720**	https://github.com/digitalbazaar/forge/blob/master/CHANGELOG.md	A-DIG-FORG-180920/63
Djangoproject					
django					
Incorrect Default Permissions	01-Sep-20	5	An issue was discovered in Django 2.2 before 2.2.16, 3.0 before 3.0.10, and 3.1 before 3.1.1 (when Python 3.7+ is used). FILE_UPLOAD_DIRECTORY_PERMISSIONS mode was not applied to intermediate-level directories created in the process of uploading files. It was also not applied to intermediate-level collected static directories when using the collectstatic management command. **CVE ID : CVE-2020-24583**	N/A	A-DJA-DJAN-180920/64
Incorrect Default Permissions	01-Sep-20	5	An issue was discovered in Django 2.2 before 2.2.16, 3.0 before 3.0.10, and 3.1 before 3.1.1 (when Python 3.7+ is used). The intermediate-level directories of the filesystem cache had the system's standard umask rather than	N/A	A-DJA-DJAN-180920/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0o077. **CVE ID : CVE-2020-24584**		
Dolibarr					
dolibarr					
Unrestricted Upload of File with Dangerous Type	02-Sep-20	6.5	Dolibarr before 11.0.5 allows low-privilege users to upload files of dangerous types, leading to arbitrary code execution. This occurs because .pht and .phar files can be uploaded. Also, a .htaccess file can be uploaded to reconfigure access control (e.g., to let .noexe files be executed as PHP code to defeat the .noexe protection mechanism). **CVE ID : CVE-2020-14209**	https://github.com/Dolibarr/dolibarr/releases/tag/11.0.5	A-DOL-DOLI-180920/66
dot-notes_project					
dot-notes					
Improper Input Validation	01-Sep-20	7.5	All versions of package dot-notes are vulnerable to Prototype Pollution via the create function. **CVE ID : CVE-2020-7717**	N/A	A-DOT-DOT--180920/67
duffel					
paginator					
Improper Control of Generation of Code ('Code Injection')	01-Sep-20	7.5	There is a vulnerability in Paginator (Elixir/Hex package) which makes it susceptible to Remote Code Execution (RCE) attacks via input parameters to the paginate() function. This will potentially affect all current users of Paginator prior to version 1.0.0. The	https://github.com/duffelhq/paginator/blob/ccf0f37fa96347cc8c8a7e9eb2c64462cec4b2dc/README.md#security-	A-DUF-PAGI-180920/68

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been patched in version 1.0.0 and all users should upgrade to this version immediately. Note that this patched version uses a dependency that requires an Elixir version >=1.5. **CVE ID : CVE-2020-15150**	consideratio ns, https://githu b.com/duffel hq/paginator /commit/bf4 5e92602e51 7c75aea046 5efc35cd661 d9ebf8, https://hex.p m/packages/ paginator	
ecommerce-codeigniter-bootstrap_project					
ecommerce-codeigniter-bootstrap					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/admin/v iews/advanced_settings/admi nUsers.php. **CVE ID : CVE-2020-25086**	N/A	A-ECO-ECOM-180920/69
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/admin/v iews/advanced_settings/langu ages.php. **CVE ID : CVE-2020-25087**	N/A	A-ECO-ECOM-180920/70
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/admin/v iews/blog/blogpublish.php. **CVE ID : CVE-2020-25088**	N/A	A-ECO-ECOM-180920/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/admin/views/ecommerce/discounts.php. **CVE ID : CVE-2020-25089**	N/A	A-ECO-ECOM-180920/72
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/admin/views/ecommerce/publish.php. **CVE ID : CVE-2020-25090**	N/A	A-ECO-ECOM-180920/73
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/vendor/views/add_product.php. **CVE ID : CVE-2020-25091**	N/A	A-ECO-ECOM-180920/74
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in _parts/header.php, within application/views/templates/clothesshop, application/views/templates/greenlabel, and application/views/templates/redlabel. **CVE ID : CVE-2020-25092**	N/A	A-ECO-ECOM-180920/75
Improper Neutralization of Input During Web	03-Sep-20	4.3	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in blog.php. within application/views/templates/	N/A	A-ECO-ECOM-180920/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			clothesshop, application/views/templates/onepage, and application/views/templates/redlabel. **CVE ID : CVE-2020-25093**		
enghouse					
web_chat					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	Enghouse Web Chat 6.2.284.34 allows XSS. When one enters their own domain name in the WebServiceLocation parameter, the response from the POST request is displayed, and any JavaScript returned from the external server is executed in the browser. This is related to CVE-2019-16951. **CVE ID : CVE-2020-13972**	N/A	A-ENG-WEB_-180920/77
eramba					
eramba					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	3.5	eramba c2.8.1 and Enterprise before e2.19.3 allows XSS via a crafted filename for a file attached to an object. For example, the filename has a complete XSS payload followed by the .png extension. **CVE ID : CVE-2020-25104**	N/A	A-ERA-ERAM-180920/78
Weak Password Recovery Mechanism for Forgotten	03-Sep-20	5	eramba c2.8.1 and Enterprise before e2.19.3 has a weak password recovery token (createHash has only a million possibilities). **CVE ID : CVE-2020-25105**	N/A	A-ERA-ERAM-180920/79

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Password					
Erlang					
rebar3					
N/A	02-Sep-20	10	Rebar3 versions 3.0.0-beta.3 to 3.13.2 are vulnerable to OS command injection via URL parameter of dependency specification. **CVE ID : CVE-2020-13802**	N/A	A-ERL-REBA-180920/80
fabbricadigitale					
multiux					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	A post-authenticated stored XSS was found in MultiUx v.3.1.12.0 via the /multiux/SaveMailbox LastName field. **CVE ID : CVE-2020-17458**	N/A	A-FAB-MULT-180920/81
Facebook					
hermes					
Access of Resource Using Incompatible Type ('Type Confusion')	04-Sep-20	6.8	A type confusion vulnerability when resolving properties of JavaScript objects with specially-crafted prototype chains in Facebook Hermes prior to commit fe52854cdf6725c2eaa9e125995da76e6ceb27da allows attackers to potentially execute arbitrary code via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications	https://github.com/facebook/hermes/commit/fe52854cdf6725c2eaa9e125995da76e6ceb27da, https://www.facebook.com/security/advisories/cve-2020-1911	A-FAC-HERM-180920/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are not affected. **CVE ID : CVE-2020-1911**		
Out-of-bounds Write	09-Sep-20	6.8	An out-of-bounds read/write vulnerability when executing lazily compiled inner generator functions in Facebook Hermes prior to commit 091835377369c8fd5917d9b87acffa721ad2a168 allows attackers to potentially execute arbitrary code via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2020-1912**	https://github.com/facebook/hermes/commit/091835377369c8fd5917d9b87acffa721ad2a168, https://www.facebook.com/security/advisories/cve-2020-1912	A-FAC-HERM-180920/83
Incorrect Conversion between Numeric Types	09-Sep-20	6.8	An Integer signedness error in the JavaScript Interpreter in Facebook Hermes prior to commit 2c7af7ec481ceffd0d14ce2d7c045e475fd71dc6 allows attackers to cause a denial of service attack or a potential RCE via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2020-1913**	https://github.com/facebook/hermes/commit/2c7af7ec481ceffd0d14ce2d7c045e475fd71dc6, https://www.facebook.com/security/advisories/cve-2020-1913	A-FAC-HERM-180920/84
forlogic					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qualiex					
Incorrect Permission Assignment for Critical Resource	02-Sep-20	6.5	ForLogic Qualiex v1 and v3 allows any authenticated customer to achieve privilege escalation via user creations, password changes, or user permission updates. **CVE ID : CVE-2020-24028**	N/A	A-FOR-QUAL-180920/85
Improper Authentication	02-Sep-20	7.5	Because of unauthenticated password changes in ForLogic Qualiex v1 and v3, customer and admin permissions and data can be accessed via a simple request. **CVE ID : CVE-2020-24029**	N/A	A-FOR-QUAL-180920/86
Operation on a Resource after Expiration or Release	02-Sep-20	7.5	ForLogic Qualiex v1 and v3 has weak token expiration. This allows remote unauthenticated privilege escalation and access to sensitive data via token reuse. **CVE ID : CVE-2020-24030**	N/A	A-FOR-QUAL-180920/87
Foxitsoftware					
phantompdf					
Insufficient Verification of Data Authenticity	04-Sep-20	5.8	In Foxit Reader and PhantomPDF before 10.0.1, and PhantomPDF before 9.7.3, attackers can obtain sensitive information about an uninitialized object because of direct transformation from PDF Object to Stream without concern for a crafted XObject. **CVE ID : CVE-2020-11493**	N/A	A-FOX-PHAN-180920/88
Out-of-bounds Write	04-Sep-20	6.8	In Foxit Reader and PhantomPDF before 10.0.1, and PhantomPDF before 9.7.3,	N/A	A-FOX-PHAN-180920/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers can execute arbitrary code via a heap-based buffer overflow because dirty image-resource data is mishandled. **CVE ID : CVE-2020-12248**		
reader					
Insufficient Verification of Data Authenticity	04-Sep-20	5.8	In Foxit Reader and PhantomPDF before 10.0.1, and PhantomPDF before 9.7.3, attackers can obtain sensitive information about an uninitialized object because of direct transformation from PDF Object to Stream without concern for a crafted XObject. **CVE ID : CVE-2020-11493**	N/A	A-FOX-READ-180920/90
Out-of-bounds Write	04-Sep-20	6.8	In Foxit Reader and PhantomPDF before 10.0.1, and PhantomPDF before 9.7.3, attackers can execute arbitrary code via a heap-based buffer overflow because dirty image-resource data is mishandled. **CVE ID : CVE-2020-12248**	N/A	A-FOX-READ-180920/91
gammautils_project					
gammautils					
Improper Input Validation	01-Sep-20	7.5	All versions of package gammautils are vulnerable to Prototype Pollution via the deepSet and deepMerge functions. **CVE ID : CVE-2020-7718**	N/A	A-GAM-GAMM-180920/92
gedi_project					
gedi					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	01-Sep-20	7.5	All versions of package gedi are vulnerable to Prototype Pollution via the set function. **CVE ID : CVE-2020-7727**	N/A	A-GED-GEDI-180920/93
Get-simple					
getsimple_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	4.3	A Reflected Cross-Site Scripting (XSS) vulnerability in GetSimple CMS v3.3.16, in the admin/index.php login portal webpage, allows remote attackers to execute JavaScript code in the client's browser and harvest login credentials after a client clicks a link, enters credentials, and submits the login form. **CVE ID : CVE-2020-23839**	N/A	A-GET-GETS-180920/94
gmapfp					
gmapfp					
Incorrect Default Permissions	01-Sep-20	5	gmapfp.org Joomla Component GMapFP J3.30pro is affected by Insecure Permissions. An attacker can access the upload function without authenticating to the application and also can upload files due the issues of unrestricted file uploads which can be bypassed by changing the content-type and name file too double extensions. **CVE ID : CVE-2020-23971**	N/A	A-GMA-GMAP-180920/95
GNU					
gnutls					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Sep-20	5	An issue was discovered in GnuTLS before 3.6.15. A server can trigger a NULL pointer dereference in a TLS 1.3 client if a no_renegotiation alert is sent with unexpected timing, and then an invalid second handshake occurs. The crash happens in the application's error handling path, where the gnutls_deinit function is called after detecting a handshake failure. **CVE ID : CVE-2020-24659**	https://security.netapp.com/advisory/ntap-20200911-0006/	A-GNU-GNUT-180920/96
Gnupg					
gnupg					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-20	6.8	GnuPG 2.2.21 and 2.2.22 (and Gpg4win 3.1.12) has an array overflow, leading to a crash or possibly unspecified other impact, when a victim imports an attacker's OpenPGP key, and this key has AEAD preferences. The overflow is caused by a g10/key-check.c error. NOTE: GnuPG 2.3.x is unaffected. GnuPG 2.2.23 is a fixed version. **CVE ID : CVE-2020-25125**	N/A	A-GNU-GNUP-180920/97
Golang					
go					
Improper Neutralization of Input During Web Page Generation ('Cross-site	02-Sep-20	4.3	Go before 1.14.8 and 1.15.x before 1.15.1 allows XSS because text/html is the default for CGI/FCGI handlers that lack a Content-Type header.	N/A	A-GOL-GO-180920/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID : CVE-2020-24553**		
Gpg4win					
gpg4win					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-20	6.8	GnuPG 2.2.21 and 2.2.22 (and Gpg4win 3.1.12) has an array overflow, leading to a crash or possibly unspecified other impact, when a victim imports an attacker's OpenPGP key, and this key has AEAD preferences. The overflow is caused by a g10/key-check.c error. NOTE: GnuPG 2.3.x is unaffected. GnuPG 2.2.23 is a fixed version. **CVE ID : CVE-2020-25125**	N/A	A-GPG-GPG4-180920/99
gruntjs					
grunt					
N/A	03-Sep-20	4.6	The package grunt before 1.3.0 are vulnerable to Arbitrary Code Execution due to the default usage of the function load() instead of its secure replacement safeLoad() of the package js-yaml inside grunt.file.readYAML. **CVE ID : CVE-2020-7729**	https://github.com/gruntjs/grunt/blob/master/lib/grunt/file.js%23L249, https://github.com/gruntjs/grunt/commit/e350cea1724eb3476464561a380fb6a64e61e4e7, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-607922,	A-GRU-GRUN-180920/100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://snyk.io/vuln/SNYK-JS-GRUNT-597546	
guidesmiths					
worksmith					
Improper Input Validation	01-Sep-20	7.5	All versions of package worksmith are vulnerable to Prototype Pollution via the setValue function. **CVE ID : CVE-2020-7725**	N/A	A-GUI-WORK-180920/101
Health					
covidsafe					
Incorrect Authorization	09-Sep-20	2.9	In the COVIDSafe application through 1.0.21 for Android, unsafe use of the Bluetooth transport option in the GATT connection allows attackers to trick the application into establishing a connection over Bluetooth BR/EDR transport, which reveals the public Bluetooth address of the victim's phone without authorisation, bypassing the Bluetooth address randomisation protection in the user's phone. **CVE ID : CVE-2020-14292**	N/A	A-HEA-COVI-180920/102
heybbs_project					
heybbs					
Improper Neutralization of Special Elements used in an	03-Sep-20	7.5	Heybbs v1.2 has a SQL injection vulnerability in login.php file via the username parameter which may allow a remote attacker to execute arbitrary code.	N/A	A-HEY-HEYB-180920/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			**CVE ID : CVE-2020-25006**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Sep-20	7.5	Heybbs v1.2 has a SQL injection vulnerability in user.php file via the ID parameter which may allow a remote attacker to execute arbitrary code. **CVE ID : CVE-2020-25004**	N/A	A-HEY-HEYB-180920/104
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Sep-20	7.5	Heybbs v1.2 has a SQL injection vulnerability in msg.php file via the ID parameter which may allow a remote attacker to execute arbitrary code. **CVE ID : CVE-2020-25005**	N/A	A-HEY-HEYB-180920/105
hyland					
onbase					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Sep-20	5	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. Directory traversal exists for writing to files, as demonstrated by the FileName parameter. **CVE ID : CVE-2020-25247**	N/A	A-HYL-ONBA-180920/106
Improper Limitation of a Pathname	11-Sep-20	5	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. Directory	N/A	A-HYL-ONBA-180920/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			traversal exists for reading files, as demonstrated by the FileName parameter. **CVE ID : CVE-2020-25248**		
N/A	11-Sep-20	5	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. The server typically logs activity only when a client application specifies that logging is desired. This can be problematic for use cases in a regulated industry, where server-side logging is required in additional situations. **CVE ID : CVE-2020-25249**	N/A	A-HYL-ONBA-180920/108
N/A	11-Sep-20	5	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. Client applications can write arbitrary data to the server logs. **CVE ID : CVE-2020-25250**	N/A	A-HYL-ONBA-180920/109
Incorrect Authorization	11-Sep-20	6.4	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. Client-side authentication is used for critical functions such as adding users or retrieving sensitive information. **CVE ID : CVE-2020-25251**	N/A	A-HYL-ONBA-180920/110
Cross-Site Request Forgery	11-Sep-20	6.8	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through	N/A	A-HYL-ONBA-180920/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			19.8.9.1000. CSRF can be used to log in a user, and then perform actions, because there are default credentials (the wstinol password for the manager or hsi account). **CVE ID : CVE-2020-25252**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Sep-20	7.5	An issue was discovered in Hyland OnBase through 18.0.0.32. It allows SQL injection, as demonstrated by the TableName, ColumnName, Name, UserId, or Password parameter. **CVE ID : CVE-2020-25253**	N/A	A-HYL-ONBA-180920/112
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Sep-20	7.5	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. It allows SQL injection, as demonstrated by TestConnection_LocalOrLinkedServer, CreateFilterFriendlyView, or AddWorkViewLinkedServer. **CVE ID : CVE-2020-25254**	N/A	A-HYL-ONBA-180920/113
N/A	11-Sep-20	5	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. It allows remote attackers to cause a denial of service (outage of connection-request processing) via a long user ID, which triggers an exception and a large log entry. **CVE ID : CVE-2020-25255**	N/A	A-HYL-ONBA-180920/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	11-Sep-20	6.4	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. PKI certificates have a private key that is the same across different customers' installations. **CVE ID : CVE-2020-25256**	N/A	A-HYL-ONBA-180920/115
Improper Restriction of XML External Entity Reference ('XXE')	11-Sep-20	7.5	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. It allows XXE attacks for read/write access to arbitrary files. **CVE ID : CVE-2020-25257**	N/A	A-HYL-ONBA-180920/116
Deserialization of Untrusted Data	11-Sep-20	7.5	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. It uses ASP.NET BinaryFormatter.Deserialize in a manner that allows attackers to transmit and execute bytecode in SOAP messages. **CVE ID : CVE-2020-25258**	N/A	A-HYL-ONBA-180920/117
Deserialization of Untrusted Data	11-Sep-20	7.5	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. It uses XML deserialization libraries in an unsafe manner. **CVE ID : CVE-2020-25259**	N/A	A-HYL-ONBA-180920/118
Deserialization of Untrusted Data	11-Sep-20	7.5	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. It allows remote attackers to execute arbitrary code because of unsafe JSON	N/A	A-HYL-ONBA-180920/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deserialization. **CVE ID : CVE-2020-25260**		
IBM					
rational_team_concert					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 182397. **CVE ID : CVE-2020-4522**	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/120
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 181122. **CVE ID : CVE-2020-4445**	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/121
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to credentials disclosure within a trusted session. IBM X-Force ID: 183314. **CVE ID : CVE-2020-4546**		
spectrum_protect_operations_center					
Improper Input Validation	02-Sep-20	7.5	IBM Spectrum Protect Operations Center 7.1.0.000 through 7.1.10 and 8.1.0.000 through 8.1.9 may allow an attacker to execute arbitrary code on the system, caused by improper validation of data prior to export. IBM X-Force ID: 186782. **CVE ID : CVE-2020-4693**	https://www.ibm.com/support/pages/node/6325341	A-IBM-SPEC-180920/123
spectrum_protect_plus					
Unrestricted Upload of File with Dangerous Type	15-Sep-20	6	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 Administrative Console could allow an authenticated attacker to upload arbitrary files which could be execute arbitrary code on the vulnerable server. This vulnerability is due to an incomplete fix for CVE-2020-4470. IBM X-Force ID: 187188. **CVE ID : CVE-2020-4703**	https://www.ibm.com/support/pages/node/6328867	A-IBM-SPEC-180920/124
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Sep-20	4	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	https://www.ibm.com/support/pages/node/6328867	A-IBM-SPEC-180920/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 187501. **CVE ID : CVE-2020-4711**		
tivoli_business_service_manager					
Insecure Storage of Sensitive Information	15-Sep-20	2.1	IBM Tivoli Business Service Manager 6.2.0.0 - 6.2.0.2 IF 1 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 178247. **CVE ID : CVE-2020-4344**	https://www.ibm.com/support/pages/node/6332437	A-IBM-TIVO-180920/126
eni					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 182397. **CVE ID : CVE-2020-4522**	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENI-180920/127
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 181122. **CVE ID : CVE-2020-4445**	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENI-180920/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 183314. **CVE ID : CVE-2020-4546**	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENI-180920/129
aspera_connect					
Untrusted Search Path	04-Sep-20	9.3	IBM Aspera Connect 3.9.9 could allow a remote attacker to execute arbitrary code on the system, caused by improper loading of Dynamic Link Libraries by the import feature. By persuading a victim to open a specially-crafted .DLL file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183190. **CVE ID : CVE-2020-4545**	https://www.ibm.com/support/pages/node/6326537	A-IBM-ASPE-180920/130
doors_next					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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	https://www.ibm.com/support/pages/node/6325343	A-IBM-DOOR-180920/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session. IBM X-Force ID: 182397. **CVE ID : CVE-2020-4522**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 181122. **CVE ID : CVE-2020-4445**	https://www.ibm.com/support/pages/node/6325343	A-IBM-DOOR-180920/132
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 183314. **CVE ID : CVE-2020-4546**	https://www.ibm.com/support/pages/node/6325343	A-IBM-DOOR-180920/133
api_connect					
N/A	03-Sep-20	4.3	IBM API Connect 2018.4.1.0 through 2018.4.1.12 could allow an attacker to launch phishing attacks by tricking the server to generate user registration emails that contain malicious URLs. IBM X-Force ID: 177933.	https://www.ibm.com/support/pages/node/6324763	A-IBM-API_-180920/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4337		
Improper Privilege Management	03-Sep-20	6.5	IBM API Connect's API Manager 2018.4.1.0 through 2018.4.1.12 is vulnerable to privilege escalation. An invitee to an API Provider organization can escalate privileges by manipulating the invitation link. IBM X-Force ID: 185508. **CVE ID : CVE-2020-4638**	https://www.ibm.com/support/pages/node/6324751	A-IBM-API_-180920/135
websphere_application_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 184433. **CVE ID : CVE-2020-4578**	https://www.ibm.com/support/pages/node/6328895	A-IBM-WEBS-180920/136
maximo_asset_management					
Deserialization of Untrusted Data	15-Sep-20	9	IBM Maximo Asset Management 7.6.0 and 7.6.1 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unsafe deserialization in Java. By sending specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID:	https://www.ibm.com/support/pages/node/6332587	A-IBM-MAXI-180920/137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			182396. **CVE ID : CVE-2020-4521**		
Cross-Site Request Forgery (CSRF)	15-Sep-20	4.3	IBM Maximo Asset Management 7.6.0 and 7.6.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 182436. **CVE ID : CVE-2020-4526**	https://www.ibm.com/support/pages/node/6332589	A-IBM-MAXI-180920/138
rational_collaborative_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 182397. **CVE ID : CVE-2020-4522**	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/139
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 181122.	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4445		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 183314. **CVE ID : CVE-2020-4546**	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/141
rational_doors_next_generation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 182397. **CVE ID : CVE-2020-4522**	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/142
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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:	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			181122. **CVE ID : CVE-2020-4445**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 183314. **CVE ID : CVE-2020-4546**	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/144
rational_engineering_lifecycle_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 182397. **CVE ID : CVE-2020-4522**	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/145
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure within a trusted session. IBM X-Force ID: 181122. **CVE ID : CVE-2020-4445**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 183314. **CVE ID : CVE-2020-4546**	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/147
rational_quality_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 182397. **CVE ID : CVE-2020-4522**	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/148
Improper Neutralization of Input During Web Page Generation ('Cross-site	02-Sep-20	3.5	IBM Jazz Team Server based Applications are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 181122. **CVE ID : CVE-2020-4445**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 183314. **CVE ID : CVE-2020-4546**	https://www.ibm.com/support/pages/node/6325343	A-IBM-RATI-180920/150
infosphere_information_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-20	3.5	IBM InfoSphere Information Server 11.7 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 187187. **CVE ID : CVE-2020-4702**	https://www.ibm.com/support/pages/node/6323721	A-IBM-INFO-180920/151
business_automation_workflow					
Improper Neutralization of Input During Web	08-Sep-20	3.5	IBM Business Process Manager 8.5, 8.6 and IBM Business Automation Workflow 18.0, 19.0, and 20.0	https://www.ibm.com/support/pages/node/6326	A-IBM-BUSI-180920/152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			are 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: 182371. **CVE ID : CVE-2020-4516**	901	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Sep-20	3.5	IBM Business Automation Workflow C.D.0 and IBM Business Process Manager 8.0, 8.5, and 8.6 are 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-ForceID: 182714. **CVE ID : CVE-2020-4530**	https://www.ibm.com/support/pages/node/6332417	A-IBM-BUSI-180920/153
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Sep-20	3.5	IBM Business Process Manager 8.5, 8.6 and IBM Business Automation Workflow 18.0, 19.0, and 20.0 are vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted	https://www.ibm.com/support/pages/node/6326825	A-IBM-BUSI-180920/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session. IBM X-Force ID: 186841. **CVE ID : CVE-2020-4698**		
business_process_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Sep-20	3.5	IBM Business Process Manager 8.5, 8.6 and IBM Business Automation Workflow 18.0, 19.0, and 20.0 are 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: 182371. **CVE ID : CVE-2020-4516**	https://www.ibm.com/support/pages/node/6326901	A-IBM-BUSI-180920/155
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Sep-20	3.5	IBM Business Automation Workflow C.D.0 and IBM Business Process Manager 8.0, 8.5, and 8.6 are 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-ForceID: 182714. **CVE ID : CVE-2020-4530**	https://www.ibm.com/support/pages/node/6332417	A-IBM-BUSI-180920/156
Improper Neutralization of Input During Web	08-Sep-20	3.5	IBM Business Process Manager 8.5, 8.6 and IBM Business Automation Workflow 18.0, 19.0, and 20.0	https://www.ibm.com/support/pages/node/6326	A-IBM-BUSI-180920/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			are vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186841. **CVE ID : CVE-2020-4698**	825	
infosphere_metadata_asset_manager					
Server-Side Request Forgery (SSRF)	04-Sep-20	4	IBM InfoSphere Metadata Asset Manager 11.7 is vulnerable to server-side request forgery. By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to submit or control server requests. IBM X-Force ID: 185416. **CVE ID : CVE-2020-4632**	https://www.ibm.com/support/pages/node/6323721	A-IBM-INFO-180920/158
engineering_test_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 182397. **CVE ID : CVE-2020-4522**	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENGI-180920/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 181122. **CVE ID : CVE-2020-4445**	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENGI-180920/160
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 183314. **CVE ID : CVE-2020-4546**	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENGI-180920/161
engineering_workflow_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 182397.	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENGI-180920/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4522		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 181122. **CVE ID : CVE-2020-4445**	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENGI-180920/163
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 183314. **CVE ID : CVE-2020-4546**	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENGI-180920/164
engineering_requirements_management_doors_next					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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:	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENGI-180920/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			182397. **CVE ID : CVE-2020-4522**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 181122. **CVE ID : CVE-2020-4445**	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENGI-180920/166
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	3.5	IBM Jazz Team Server based Applications are 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: 183314. **CVE ID : CVE-2020-4546**	https://www.ibm.com/support/pages/node/6325343	A-IBM-ENGI-180920/167
Igniterealtime					
openfire					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	4.3	In Ignite Realtime Openfire 4.5.1 a Stored Cross-site Vulnerability allows an attacker to execute an arbitrary malicious URL via the vulnerable POST parameter searchName", "alias" in the import certificate	N/A	A-IGN-OPEN-180920/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			trusted page **CVE ID : CVE-2020-24601**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	4.3	Ignite Realtime Openfire 4.5.1 has a reflected Cross-site scripting vulnerability which allows an attacker to execute arbitrary malicious URL via the vulnerable GET parameter searchName", "searchValue", "searchDescription", "searchDefaultValue","searchPlugin", "searchDescription" and "searchDynamic" in the Server Properties and Security Audit Viewer JSP page **CVE ID : CVE-2020-24602**	N/A	A-IGN-OPEN-180920/169
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-20	4.3	A Reflected XSS vulnerability was discovered in Ignite Realtime Openfire version 4.5.1. The XSS vulnerability allows remote attackers to inject arbitrary web script or HTML via the GET request "searchName", "searchValue", "searchDescription", "searchDefaultValue","searchPlugin", "searchDescription" and "searchDynamic" in server-properties.jsp and security-audit-viewer.jsp **CVE ID : CVE-2020-24604**	N/A	A-IGN-OPEN-180920/170
inspircd					
inspircd					
Use After Free	11-Sep-20	6.8	An issue was discovered in InspIRCd 2 before 2.0.29 and 3 before 3.6.0. The pgsql module contains a use after free vulnerability. When combined	N/A	A-INS-INSP-180920/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with the sqlauth or sqloper modules, this vulnerability can be used for remote crashing of an InspIRCd server by any user able to connect to a server. **CVE ID : CVE-2020-25269**		
Intel					
standard_manageability					
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	7.5	Improper buffer restrictions in network subsystem in provisioned Intel(R) AMT and Intel(R) ISM versions before 11.8.79, 11.12.79, 11.22.79, 12.0.68 and 14.0.39 may allow an unauthenticated user to potentially enable escalation of privilege via network access. On un-provisioned systems, an authenticated user may potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-8758**	https://security.netapp.com/advisory/ntap-20200911-0005/	A-INT-STAN-180920/172
active_management_technology					
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	7.5	Improper buffer restrictions in network subsystem in provisioned Intel(R) AMT and Intel(R) ISM versions before 11.8.79, 11.12.79, 11.22.79, 12.0.68 and 14.0.39 may allow an unauthenticated user to potentially enable escalation of privilege via network access. On un-provisioned systems, an authenticated user may potentially enable escalation of privilege via local	https://security.netapp.com/advisory/ntap-20200911-0005/	A-INT-ACTI-180920/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access. **CVE ID : CVE-2020-8758**		
invertase					
deeps					
Improper Input Validation	01-Sep-20	7.5	All versions of package deeps are vulnerable to Prototype Pollution via the set function. **CVE ID : CVE-2020-7716**	N/A	A-INV-DEEP-180920/174
Jenkins					
cadence_vmanager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	Jenkins Cadence vManager Plugin 3.0.4 and earlier does not escape build descriptions in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Run/Update permission. **CVE ID : CVE-2020-2243**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1936	A-JEN-CADE-180920/175
parameterized_remote_trigger					
Missing Encryption of Sensitive Data	01-Sep-20	4	Jenkins Parameterized Remote Trigger Plugin 3.1.3 and earlier stores a secret unencrypted in its global configuration file on the Jenkins controller where it can be viewed by attackers with access to the Jenkins controller file system. **CVE ID : CVE-2020-2239**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1625	A-JEN-PARA-180920/176
database					
Cross-Site Request Forgery (CSRF)	01-Sep-20	6.8	A cross-site request forgery (CSRF) vulnerability in Jenkins database Plugin 1.6 and earlier allows attackers to execute arbitrary SQL scripts.	https://jenkins.io/security/advisory/2020-09-01/#SECURI	A-JEN-DATA-180920/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-2240	TY-1023	
Cross-Site Request Forgery (CSRF)	01-Sep-20	6.8	A cross-site request forgery (CSRF) vulnerability in Jenkins database Plugin 1.6 and earlier allows attackers to connect to an attacker-specified database server using attacker-specified credentials. **CVE ID : CVE-2020-2241**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1024	A-JEN-DATA-180920/178
Missing Authorization	01-Sep-20	4	A missing permission check in Jenkins database Plugin 1.6 and earlier allows attackers with Overall/Read access to Jenkins to connect to an attacker-specified database server using attacker-specified credentials. **CVE ID : CVE-2020-2242**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1024	A-JEN-DATA-180920/179
build_failure_analyzer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	Jenkins Build Failure Analyzer Plugin 1.27.0 and earlier does not escape matching text in a form validation response, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers able to provide console output for builds used to test build log indications. **CVE ID : CVE-2020-2244**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1770	A-JEN-BUIL-180920/180
valgrind					
Improper Restriction of XML External Entity Reference	01-Sep-20	5.5	Jenkins Valgrind Plugin 0.28 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2020-2245**	https://jenkins.io/security/advisory/2020-09-01/#SECURI	A-JEN-VALG-180920/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('XXE')				TY-1829	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	Jenkins Valgrind Plugin 0.28 and earlier does not escape content in Valgrind XML reports, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control Valgrind XML report contents. **CVE ID : CVE-2020-2246**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1830	A-JEN-VALG-180920/182
klocwork_analysis					
Improper Restriction of XML External Entity Reference ('XXE')	01-Sep-20	4	Jenkins Klocwork Analysis Plugin 2020.2.1 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2020-2247**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1831	A-JEN-KLOC-180920/183
jsgames					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	4.3	Jenkins JSGames Plugin 0.2 and earlier evaluates part of a URL as code, resulting in a reflected cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2020-2248**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1905	A-JEN-JSGA-180920/184
team_foundation_server					
Missing Encryption of Sensitive Data	01-Sep-20	2.1	Jenkins Team Foundation Server Plugin 5.157.1 and earlier stores a webhook secret unencrypted in its global configuration file on the Jenkins controller where it can be viewed by attackers with access to the Jenkins controller file system.	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1506	A-JEN-TEAM-180920/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-2249		
soapui_pro_functional_testing					
Missing Encryption of Sensitive Data	01-Sep-20	4	Jenkins SoapUI Pro Functional Testing Plugin 1.3 and earlier stores project passwords unencrypted in job config.xml files on the Jenkins controller where they can be viewed by attackers with Extended Read permission, or access to the Jenkins controller file system. **CVE ID : CVE-2020-2250**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1631%20(1)	A-JEN-SOAP-180920/186
Cleartext Transmission of Sensitive Information	01-Sep-20	4	Jenkins SoapUI Pro Functional Testing Plugin 1.5 and earlier transmits project passwords in its configuration in plain text as part of job configuration forms, potentially resulting in their exposure. **CVE ID : CVE-2020-2251**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1631%20(2)	A-JEN-SOAP-180920/187
jenkins					
Cleartext Transmission of Sensitive Information	01-Sep-20	4	Jenkins SoapUI Pro Functional Testing Plugin 1.5 and earlier transmits project passwords in its configuration in plain text as part of job configuration forms, potentially resulting in their exposure. **CVE ID : CVE-2020-2251**	https://jenkins.io/security/advisory/2020-09-01/#SECURITY-1631%20(2)	A-JEN-JENK-180920/188
git_parameter					
Improper Neutralization of Input During Web Page	01-Sep-20	3.5	Jenkins Git Parameter Plugin 0.9.12 and earlier does not escape the repository field on the 'Build with Parameters' page, resulting in a stored	https://jenkins.io/security/advisory/2020-09-01/#SECURI	A-JEN-GIT_-180920/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission. **CVE ID : CVE-2020-2238**	TY-1884	
johnkerl					
miller					
Improper Control of Generation of Code ('Code Injection')	02-Sep-20	4.4	In Miller (command line utility) using the configuration file support introduced in version 5.9.0, it is possible for an attacker to cause Miller to run arbitrary code by placing a malicious `.mlrrc` file in the working directory. See linked GitHub Security Advisory for complete details. A fix is ready and will be released as Miller 5.9.1. **CVE ID : CVE-2020-15167**	https://github.com/johnkerl/miller/security/advisories/GHSA-mw2v-4q78-j2cw	A-JOH-MILL-180920/190
Kaspersky					
vpn_secure_connection					
N/A	02-Sep-20	3.6	The installer of Kaspersky VPN Secure Connection prior to 5.0 was vulnerable to arbitrary file deletion that could allow an attacker to delete any file in the system. **CVE ID : CVE-2020-25043**	N/A	A-KAS-VPN_-180920/191
virus_removal_tool					
N/A	02-Sep-20	3.6	Kaspersky Virus Removal Tool (KVRT) prior to 15.0.23.0 was vulnerable to arbitrary file corruption that could provide an attacker with the opportunity to eliminate content of any file in the	N/A	A-KAS-VIRU-180920/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system. **CVE ID : CVE-2020-25044**		
security_center					
Uncontrolled Search Path Element	02-Sep-20	4.4	Installers of Kaspersky Security Center and Kaspersky Security Center Web Console prior to 12 & prior to 12 Patch A were vulnerable to a DLL hijacking attack that allowed an attacker to elevate privileges in the system. **CVE ID : CVE-2020-25045**	N/A	A-KAS-SECU-180920/193
security_center_web_console					
Uncontrolled Search Path Element	02-Sep-20	4.4	Installers of Kaspersky Security Center and Kaspersky Security Center Web Console prior to 12 & prior to 12 Patch A were vulnerable to a DLL hijacking attack that allowed an attacker to elevate privileges in the system. **CVE ID : CVE-2020-25045**	N/A	A-KAS-SECU-180920/194
KDE					
ark					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Sep-20	4.3	In KDE Ark before 20.08.1, a crafted TAR archive with symlinks can install files outside the extraction directory, as demonstrated by a write operation to a user's home directory. **CVE ID : CVE-2020-24654**	https://bugzilla.suse.com/show_bug.cgi?id=1175857, https://github.com/KDE/ark/commit/8bf8c5ef07b0ac5e914d752681e470dea403a5bd, https://kde.o	A-KDE-ARK-180920/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				rg/info/security/advisory-20200827-1.txt	
Kentico					
kentico					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-20	4.3	Cross Site Scripting (XSS) vulnerability in Kentico before 12.0.75. **CVE ID : CVE-2020-24794**	N/A	A-KEN-KENT-180920/196
Laravel					
laravel					
Improper Input Validation	04-Sep-20	4.3	An issue was discovered in Laravel before 6.18.34 and 7.x before 7.23.2. Unvalidated values are saved to the database in some situations in which table names are stripped during a mass assignment. **CVE ID : CVE-2020-24940**	N/A	A-LAR-LARA-180920/197
Improper Input Validation	04-Sep-20	4.3	An issue was discovered in Laravel before 6.18.35 and 7.x before 7.24.0. The $guarded property is mishandled in some situations involving requests with JSON column nesting expressions. **CVE ID : CVE-2020-24941**	N/A	A-LAR-LARA-180920/198
libproxy_project					
libproxy					
Out-of-bounds	09-Sep-20	5	url::recvline in url.cpp in libproxy 0.4.x through 0.4.15	N/A	A-LIB-LIBP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			allows a remote HTTP server to trigger uncontrolled recursion via a response composed of an infinite stream that lacks a newline character. This leads to stack exhaustion. **CVE ID : CVE-2020-25219**		180920/199
librehealth					
librehealth_ehr					
Unrestricted Upload of File with Dangerous Type	01-Sep-20	6.5	interface/new/new_comprehensive_save.php in LibreHealth EHR 2.0.0 suffers from an authenticated file upload vulnerability, allowing remote attackers to achieve remote code execution (RCE) on the hosting webserver by uploading a maliciously crafted image. **CVE ID : CVE-2020-23829**	N/A	A-LIB-LIBR-180920/200
Liferay					
liferay_portal					
URL Redirection to Untrusted Site ('Open Redirect')	01-Sep-20	5	The redirect module in Liferay Portal before 7.3.3 does not limit the number of URLs resulting in a 404 error that is recorded, which allows remote attackers to perform a denial of service attack by making repeated requests for pages that do not exist. **CVE ID : CVE-2020-24554**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/119784956	A-LIF-LIFE-180920/201
Linuxfoundation					
the_update_framework					
Incorrect	09-Sep-20	4.9	Python TUF (The Update	https://githu	A-LIN-THE_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			Framework) reference implementation before version 0.12 it will incorrectly trust a previously downloaded root metadata file which failed verification at download time. This allows an attacker who is able to serve multiple new versions of root metadata (i.e. by a person-in-the-middle attack) culminating in a version which has not been correctly signed to control the trust chain for future updates. This is fixed in version 0.12 and newer. **CVE ID : CVE-2020-15163**	b.com/theupdateframework/tuf/commit/3d342e648fbacdf43a13d7ba8886aaaf07334af7, https://github.com/theupdateframework/tuf/security/advisories/GHSA-f8mr-jv2c-v8mg	180920/202
localization_manager_project					
localization_manager					
Missing Authorization	02-Sep-20	4	The l10nmgr (aka Localization Manager) extension before 7.4.0, 8.x before 8.7.0, and 9.x before 9.2.0 for TYPO3 allows Information Disclosure (translatable fields). **CVE ID : CVE-2020-25025**	https://typo3.org/security/advisory/typo3-ext-sa-2020-016	A-LOC-LOCA-180920/203
locutus_project					
locutus					
Improper Input Validation	01-Sep-20	7.5	Versions of package locutus before 2.0.12 are vulnerable to prototype Pollution via the php.strings.parse_str function. **CVE ID : CVE-2020-7719**	https://github.com/kvz/locutus/pull/418/	A-LOC-LOCU-180920/204
loway					
queuemetrics					
Improper Neutralizati	09-Sep-20	6.5	A SQL injection vulnerability at a tpf URI in Loway	N/A	A-LOW-QUEU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Special Elements used in an SQL Command ('SQL Injection')			QueueMetrics before 19.04.1 allows remote authenticated attackers to execute arbitrary SQL commands via the TASKS_LIST__pt.querystring parameter. **CVE ID : CVE-2020-13127**		180920/205
magmi_project					
magmi					
Cross-Site Request Forgery (CSRF)	01-Sep-20	6.8	Currently, all versions of MAGMI are vulnerable to CSRF due to the lack of CSRF tokens. RCE (via phpcli command) is possible in the event that a CSRF is leveraged against an existing admin session for MAGMI. **CVE ID : CVE-2020-5776**	N/A	A-MAG-MAGM-180920/206
Improper Authentication	01-Sep-20	7.5	MAGMI versions prior to 0.7.24 are vulnerable to a remote authentication bypass due to allowing default credentials in the event there is a database connection failure. A remote attacker can trigger this connection failure if the Mysql setting max_connections (default 151) is lower than Apache (or another web server) setting MaxRequestWorkers (formerly MaxClients) (default 256). This can be done by sending at least 151 simultaneous requests to the Magento website to trigger a "Too many connections" error, then use default	N/A	A-MAG-MAGM-180920/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			magmi:magmi basic authentication to remotely bypass authentication. **CVE ID : CVE-2020-5777**		
maracms					
maracms					
Unrestricted Upload of File with Dangerous Type	03-Sep-20	6.5	An arbitrary file upload issue exists in Mara CMS 7.5. In order to exploit this, an attacker must have a valid authenticated (admin/manager) session and make a codebase/dir.php?type=filenew request to upload PHP code to codebase/handler.php. **CVE ID : CVE-2020-25042**	N/A	A-MAR-MARA-180920/208
mbed					
mbedtls					
Information Exposure Through Discrepancy	02-Sep-20	2.1	A Lucky 13 timing side channel in mbedtls_ssl_decrypt_buf in library/ssl_msg.c in Trusted Firmware Mbed TLS through 2.23.0 allows an attacker to recover secret key information. This affects CBC mode because of a computed time difference based on a padding length. **CVE ID : CVE-2020-16150**	https://tls.mbed.org/tech-updates/security-advisories/mbedtls-security-advisory-2020-09-1	A-MBE-MBED-180920/209
Mcafee					
mvision_endpoint					
Improper Privilege Manageme	09-Sep-20	3.6	Improper Access Control vulnerability in McAfee MVISION Endpoint prior to 20.9 Update allows local users	https://kc.mcafee.com/corporate/index?page=cont	A-MCA-MVIS-180920/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nt			to bypass security mechanisms and deny access to the SYSTEM folder via incorrectly applied permissions. **CVE ID : CVE-2020-7324**	ent&id=SB10328	
Improper Link Resolution Before File Access ('Link Following')	09-Sep-20	4.6	Privilege Escalation vulnerability in McAfee MVISION Endpoint prior to 20.9 Update allows local users to access files which the user otherwise would not have access to via manipulating symbolic links to redirect McAfee file operations to an unintended file. **CVE ID : CVE-2020-7325**	https://kc.mcafee.com/corporate/index?page=content&id=SB10328	A-MCA-MVIS-180920/211
mcafee_agent					
Improper Privilege Management	10-Sep-20	6.9	Privilege Escalation vulnerability in the installer in McAfee Agent (MA) for Windows prior to 5.6.6 allows local users to assume SYSTEM rights during the installation of MA via manipulation of log files. **CVE ID : CVE-2020-7311**	https://kc.mcafee.com/corporate/index?page=content&id=SB10325	A-MCA-MCAF-180920/212
Uncontrolled Search Path Element	10-Sep-20	4.6	DLL Search Order Hijacking Vulnerability in the installer in McAfee Agent (MA) for Windows prior to 5.6.6 allows local users to execute arbitrary code and escalate privileges via execution from a compromised folder. **CVE ID : CVE-2020-7312**	https://kc.mcafee.com/corporate/index?page=content&id=SB10325	A-MCA-MCAF-180920/213
Incorrect Permission	10-Sep-20	7.2	Privilege Escalation Vulnerability in the installer in	https://kc.mcafee.com/co	A-MCA-MCAF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			McAfee Data Exchange Layer (DXL) Client for Mac shipped with McAfee Agent (MA) for Mac prior to MA 5.6.6 allows local users to run commands as root via incorrectly applied permissions on temporary files. **CVE ID : CVE-2020-7314**	rporate/index?page=content&id=SB10325	180920/214
Untrusted Search Path	10-Sep-20	4.6	DLL Injection Vulnerability in McAfee Agent (MA) for Windows prior to 5.6.6 allows local users to execute arbitrary code via careful placement of a malicious DLL. **CVE ID : CVE-2020-7315**	https://kc.mcafee.com/corporate/index?page=content&id=SB10325	A-MCA-MCAF-180920/215
endpoint_security					
Improper Link Resolution Before File Access ('Link Following')	09-Sep-20	4.6	Improper Access Control vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local users to access files which the user otherwise would not have access to via manipulating symbolic links to redirect McAfee file operations to an unintended file. **CVE ID : CVE-2020-7319**	https://kc.mcafee.com/corporate/index?page=content&id=SB10327	A-MCA-ENDP-180920/216
N/A	09-Sep-20	2.1	Protection Mechanism Failure vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local administrator to temporarily reduce the detection capability allowing	https://kc.mcafee.com/corporate/index?page=content&id=SB10327	A-MCA-ENDP-180920/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			otherwise detected malware to run via stopping certain Microsoft services. **CVE ID : CVE-2020-7320**		
Information Exposure	09-Sep-20	2.1	Information Disclosure Vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local users to gain access to sensitive information via incorrectly logging of sensitive information in debug logs. **CVE ID : CVE-2020-7322**	https://kc.mcafee.com/corporate/index?page=content&id=SB10327	A-MCA-ENDP-180920/218
Improper Authentication	09-Sep-20	5.9	Authentication Protection Bypass vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows physical local users to bypass the Windows lock screen via triggering certain detection events while the computer screen is locked and the McTray.exe is running with elevated privileges. This issue is timing dependent and requires physical access to the machine. **CVE ID : CVE-2020-7323**	https://kc.mcafee.com/corporate/index?page=content&id=SB10327	A-MCA-ENDP-180920/219
Microsoft					
365_apps					
Improper Restriction of Operations within the	11-Sep-20	6.8	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka	N/A	A-MIC-365_-180920/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1332, CVE-2020-1335, CVE-2020-1594. **CVE ID : CVE-2020-1193**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1335, CVE-2020-1594. **CVE ID : CVE-2020-1332**	N/A	A-MIC-365_-180920/221
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1332, CVE-2020-1594. **CVE ID : CVE-2020-1335**	N/A	A-MIC-365_-180920/222
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1332, CVE-2020-1335.	N/A	A-MIC-365_-180920/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1594		
office_web_apps					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1332, CVE-2020-1594. **CVE ID : CVE-2020-1335**	N/A	A-MIC-OFFI-180920/224
onedrive					
Improper Link Resolution Before File Access ('Link Following')	11-Sep-20	3.6	An elevation of privilege vulnerability exists when the OneDrive for Windows Desktop application improperly handles symbolic links, aka 'OneDrive for Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16852, CVE-2020-16853. **CVE ID : CVE-2020-16851**	N/A	A-MIC-ONED-180920/225
Improper Privilege Management	11-Sep-20	3.6	An elevation of privilege vulnerability exists when the OneDrive for Windows Desktop application improperly handles symbolic links, aka 'OneDrive for Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16851, CVE-2020-16853. **CVE ID : CVE-2020-16852**	N/A	A-MIC-ONED-180920/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	11-Sep-20	3.6	An elevation of privilege vulnerability exists when the OneDrive for Windows Desktop application improperly handles symbolic links, aka 'OneDrive for Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16851, CVE-2020-16852. **CVE ID : CVE-2020-16853**	N/A	A-MIC-ONED-180920/227
chakracore					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	9.3	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1172, CVE-2020-1180. **CVE ID : CVE-2020-1057**	N/A	A-MIC-CHAK-180920/228
edge					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	9.3	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1172, CVE-2020-1180. **CVE ID : CVE-2020-1057**	N/A	A-MIC-EDGE-180920/229
office					
Out-of-bounds	11-Sep-20	4.3	An information disclosure vulnerability exists when Microsoft Office software	N/A	A-MIC-OFFI-180920/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka 'Microsoft Office Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16855**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1332, CVE-2020-1335, CVE-2020-1594. **CVE ID : CVE-2020-1193**	N/A	A-MIC-OFFI-180920/231
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1335, CVE-2020-1594. **CVE ID : CVE-2020-1332**	N/A	A-MIC-OFFI-180920/232
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1332,	N/A	A-MIC-OFFI-180920/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1594. **CVE ID : CVE-2020-1335**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1332, CVE-2020-1335. **CVE ID : CVE-2020-1594**	N/A	A-MIC-OFFI-180920/234
sharepoint_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	4.3	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1227, CVE-2020-1482, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1345**	N/A	A-MIC-SHAR-180920/235
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1227, CVE-2020-1345, CVE-	N/A	A-MIC-SHAR-180920/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1482, CVE-2020-1575. **CVE ID : CVE-2020-1514**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	4.3	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1227, CVE-2020-1345, CVE-2020-1482, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1198**	N/A	A-MIC-SHAR-180920/237
Download of Code Without Integrity Check	11-Sep-20	7.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1210, CVE-2020-1452, CVE-2020-1453, CVE-2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1200**	N/A	A-MIC-SHAR-180920/238
Download of Code Without Integrity Check	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1452, CVE-2020-1453, CVE-	N/A	A-MIC-SHAR-180920/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1210**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1345, CVE-2020-1482, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1227**	N/A	A-MIC-SHAR-180920/240
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1332, CVE-2020-1594. **CVE ID : CVE-2020-1335**	N/A	A-MIC-SHAR-180920/241
Download of Code Without Integrity Check	11-Sep-20	7.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1210, CVE-2020-1453, CVE-2020-1576, CVE-2020-1595.	N/A	A-MIC-SHAR-180920/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1452		
Download of Code Without Integrity Check	11-Sep-20	7.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1210, CVE-2020-1452, CVE-2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1453**	N/A	A-MIC-SHAR-180920/243
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	4.3	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1227, CVE-2020-1345, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1482**	N/A	A-MIC-SHAR-180920/244
Download of Code Without Integrity Check	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1210, CVE-2020-1452, CVE-2020-1453, CVE-2020-1595.	N/A	A-MIC-SHAR-180920/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1576		
Download of Code Without Integrity Check	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft SharePoint where APIs aren't properly protected from unsafe data input, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1210, CVE-2020-1452, CVE-2020-1453, CVE-2020-1576. **CVE ID : CVE-2020-1595**	N/A	A-MIC-SHAR-180920/246
sharepoint_enterprise_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	4.3	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1227, CVE-2020-1482, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1345**	N/A	A-MIC-SHAR-180920/247
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1227, CVE-2020-1345, CVE-	N/A	A-MIC-SHAR-180920/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1482, CVE-2020-1575. **CVE ID : CVE-2020-1514**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	4.3	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1227, CVE-2020-1345, CVE-2020-1482, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1198**	N/A	A-MIC-SHAR-180920/249
Download of Code Without Integrity Check	11-Sep-20	7.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1210, CVE-2020-1452, CVE-2020-1453, CVE-2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1200**	N/A	A-MIC-SHAR-180920/250
Download of Code Without Integrity Check	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1452, CVE-2020-1453, CVE-	N/A	A-MIC-SHAR-180920/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1210**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1345, CVE-2020-1482, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1227**	N/A	A-MIC-SHAR-180920/252
Download of Code Without Integrity Check	11-Sep-20	7.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1210, CVE-2020-1453, CVE-2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1452**	N/A	A-MIC-SHAR-180920/253
Download of Code Without Integrity Check	11-Sep-20	7.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1210, CVE-2020-1452, CVE-	N/A	A-MIC-SHAR-180920/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1453**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	4.3	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1227, CVE-2020-1345, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1482**	N/A	A-MIC-SHAR-180920/255
Download of Code Without Integrity Check	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1210, CVE-2020-1452, CVE-2020-1453, CVE-2020-1595. **CVE ID : CVE-2020-1576**	N/A	A-MIC-SHAR-180920/256
Download of Code Without Integrity Check	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft SharePoint where APIs aren't properly protected from unsafe data input, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1210, CVE-2020-1452, CVE-	N/A	A-MIC-SHAR-180920/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1453, CVE-2020-1576. **CVE ID : CVE-2020-1595**		
office_online_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1332, CVE-2020-1594. **CVE ID : CVE-2020-1335**	N/A	A-MIC-OFFI-180920/258
sharepoint_foundation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	4.3	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1227, CVE-2020-1482, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1345**	N/A	A-MIC-SHAR-180920/259
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-	N/A	A-MIC-SHAR-180920/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1227, CVE-2020-1345, CVE-2020-1482, CVE-2020-1575. **CVE ID : CVE-2020-1514**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	4.3	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1227, CVE-2020-1345, CVE-2020-1482, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1198**	N/A	A-MIC-SHAR-180920/261
Download of Code Without Integrity Check	11-Sep-20	7.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1210, CVE-2020-1452, CVE-2020-1453, CVE-2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1200**	N/A	A-MIC-SHAR-180920/262
Download of Code Without Integrity Check	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-	N/A	A-MIC-SHAR-180920/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1452, CVE-2020-1453, CVE-2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1210**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1345, CVE-2020-1482, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1227**	N/A	A-MIC-SHAR-180920/264
Download of Code Without Integrity Check	11-Sep-20	7.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1210, CVE-2020-1453, CVE-2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1452**	N/A	A-MIC-SHAR-180920/265
Download of Code Without Integrity Check	11-Sep-20	7.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-	N/A	A-MIC-SHAR-180920/266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1210, CVE-2020-1452, CVE-2020-1576, CVE-2020-1595. **CVE ID : CVE-2020-1453**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	4.3	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1227, CVE-2020-1345, CVE-2020-1514, CVE-2020-1575. **CVE ID : CVE-2020-1482**	N/A	A-MIC-SHAR-180920/267
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1198, CVE-2020-1227, CVE-2020-1345, CVE-2020-1482, CVE-2020-1514. **CVE ID : CVE-2020-1575**	N/A	A-MIC-SHAR-180920/268
Download of Code Without Integrity Check	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-	N/A	A-MIC-SHAR-180920/269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1210, CVE-2020-1452, CVE-2020-1453, CVE-2020-1595. **CVE ID : CVE-2020-1576**		
Download of Code Without Integrity Check	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft SharePoint where APIs aren't properly protected from unsafe data input, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1200, CVE-2020-1210, CVE-2020-1452, CVE-2020-1453, CVE-2020-1576. **CVE ID : CVE-2020-1595**	N/A	A-MIC-SHAR-180920/270
excel					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1335, CVE-2020-1594. **CVE ID : CVE-2020-1332**	N/A	A-MIC-EXCE-180920/271
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1332, CVE-2020-1594. **CVE ID : CVE-2020-1335**	N/A	A-MIC-EXCE-180920/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	6.8	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'. This CVE ID is unique from CVE-2020-1193, CVE-2020-1332, CVE-2020-1335. **CVE ID : CVE-2020-1594**	N/A	A-MIC-EXCE-180920/273
dynamics_365					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-16859, CVE-2020-16861, CVE-2020-16864, CVE-2020-16871, CVE-2020-16872, CVE-2020-16878. **CVE ID : CVE-2020-16858**	N/A	A-MIC-DYNA-180920/274
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-16858,	N/A	A-MIC-DYNA-180920/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-16861, CVE-2020-16864, CVE-2020-16871, CVE-2020-16872, CVE-2020-16878. **CVE ID : CVE-2020-16859**		
Improper Input Validation	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft Dynamics 365 (on-premises) when the server fails to properly sanitize web requests to an affected Dynamics server, aka 'Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16862. **CVE ID : CVE-2020-16860**	N/A	A-MIC-DYNA-180920/276
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-16858, CVE-2020-16859, CVE-2020-16864, CVE-2020-16871, CVE-2020-16872, CVE-2020-16878. **CVE ID : CVE-2020-16861**	N/A	A-MIC-DYNA-180920/277
Improper Input Validation	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft Dynamics 365 (on-premises) when the server fails to properly sanitize web	N/A	A-MIC-DYNA-180920/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests to an affected Dynamics server, aka 'Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16860. **CVE ID : CVE-2020-16862**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-16858, CVE-2020-16859, CVE-2020-16861, CVE-2020-16871, CVE-2020-16872, CVE-2020-16878. **CVE ID : CVE-2020-16864**	N/A	A-MIC-DYNA-180920/279
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-16858, CVE-2020-16859, CVE-2020-16861, CVE-2020-16864, CVE-2020-16872, CVE-2020-16878.	N/A	A-MIC-DYNA-180920/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16871		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-16858, CVE-2020-16859, CVE-2020-16861, CVE-2020-16864, CVE-2020-16871, CVE-2020-16878. **CVE ID : CVE-2020-16872**	N/A	A-MIC-DYNA-180920/281
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-20	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-16858, CVE-2020-16859, CVE-2020-16861, CVE-2020-16864, CVE-2020-16871, CVE-2020-16872. **CVE ID : CVE-2020-16878**	N/A	A-MIC-DYNA-180920/282
dynamics_365_for_finance_and_operations					
Improper Input Validation	11-Sep-20	6.5	A remote code execution vulnerability exists in Microsoft Dynamics 365 for Finance and Operations (on-premises) version 10.0.11, aka	N/A	A-MIC-DYNA-180920/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16857**		
Midnightbsd					
midnightbsd					
NULL Pointer Dereference	03-Sep-20	4.9	In MidnightBSD before 1.2.6 and 1.3 before August 2020, and FreeBSD before 7, a NULL pointer dereference was found in the Linux emulation layer that allows attackers to crash the running kernel. During binary interaction, td->td_emuldata in sys/compat/linux/linux_emul.h is not getting initialized and returns NULL from em_find(). **CVE ID : CVE-2020-24385**	http://www.midnightbsd.org/security/adv/MIDNIGHTBSD-SA-20:02.txt	A-MID-MIDN-180920/284
Out-of-bounds Write	03-Sep-20	4.9	A memory corruption vulnerability was found in the kernel function kern_getfsstat in MidnightBSD before 1.2.7 and 1.3 through 2020-08-19, and FreeBSD through 11.4, that allows an attacker to trigger an invalid free and crash the system via a crafted size value in conjunction with an invalid mode. **CVE ID : CVE-2020-24863**	http://www.midnightbsd.org/security/adv/MIDNIGHTBSD-SA-20:01.txt, https://www.freebsd.org/security/advisories/FreeBSD-EN-20:18.getfsstat.asc	A-MID-MIDN-180920/285
Nagios					
nagios_xi					
Improper Privilege Manageme	09-Sep-20	10	An issue was found in Nagios XI before 5.7.3. There is a privilege escalation	https://www.nagios.com/download	A-NAG-NAGI-180920/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nt			vulnerability in backend scripts that ran as root where some included files were editable by nagios user. This issue was fixed in version 5.7.3. **CVE ID : CVE-2020-15903**	s/nagios-xi/change-log/	
Nasm					
network_assembler					
Double Free	04-Sep-20	7.5	In NASM 2.15.04rc3, there is a double-free vulnerability in pp_tokline asm/preproc.c. This is fixed in commit 8806c3ca007b84accac21dd88b900fb03614ceb7. **CVE ID : CVE-2020-24978**	N/A	A-NAS-NETW-180920/287
NEC					
expresscluster_x					
Improper Restriction of XML External Entity Reference ('XXE')	10-Sep-20	5	This vulnerability allows remote attackers to disclose sensitive information on affected installations of NEC ExpressCluster 4.1. Authentication is not required to exploit this vulnerability. The specific flaw exists within the clpwebmc executable. Due to the improper restriction of XML External Entity (XXE) references, a specially-crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the	N/A	A-NEC-EXPR-180920/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			context of SYSTEM. Was ZDI-CAN-10801. **CVE ID : CVE-2020-17408**		
Netapp					
steelstore_cloud_integrated_storage					
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	7.5	Improper buffer restrictions in network subsystem in provisioned Intel(R) AMT and Intel(R) ISM versions before 11.8.79, 11.12.79, 11.22.79, 12.0.68 and 14.0.39 may allow an unauthenticated user to potentially enable escalation of privilege via network access. On un-provisioned systems, an authenticated user may potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-8758**	https://security.netapp.com/advisory/ntap-20200911-0005/	A-NET-STEE-180920/289
clustered_data_ontap					
Incorrect Authorization	02-Sep-20	5.5	Clustered Data ONTAP versions prior to 9.3P19, 9.5P14, 9.6P9 and 9.7 are susceptible to a vulnerability which when successfully exploited could lead to addition or modification of data or disclosure of sensitive information. **CVE ID : CVE-2020-8576**	N/A	A-NET-CLUS-180920/290
nmfc					
power_line_communications					
Information Exposure Through Sent Data	01-Sep-20	3.3	All trailer Power Line Communications are affected. PLC bus traffic can be sniffed reliably via an active antenna	N/A	A-NMF-POWE-180920/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			up to 6 feet away. Further distances are also possible, subject to environmental conditions and receiver improvements. **CVE ID : CVE-2020-14514**		
nodee-utils_project					
nodee-utils					
Improper Input Validation	01-Sep-20	7.5	All versions of package nodee-utils are vulnerable to Prototype Pollution via the deepSet function. **CVE ID : CVE-2020-7722**	N/A	A-NOD-NODE-180920/292
node-oojs_project					
node-oojs					
Improper Input Validation	01-Sep-20	7.5	All versions of package node-oojs are vulnerable to Prototype Pollution via the setPath function. **CVE ID : CVE-2020-7721**	N/A	A-NOD-NODE-180920/293
noise-java_project					
noise-java					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.5	An issue was discovered in Noise-Java through 2020-08-27. ChaChaPolyCipherState.encryptWithAd() allows out-of-bounds access. **CVE ID : CVE-2020-25021**	https://github.com/rweather/noise-java/pull/12	A-NOI-NOIS-180920/294
Improper Restriction of Operations within the Bounds of a	04-Sep-20	7.5	An issue was discovered in Noise-Java through 2020-08-27. AESGCMFallbackCipherState.encryptWithAd() allows out-of-bounds access.	https://github.com/rweather/noise-java/pull/12	A-NOI-NOIS-180920/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			**CVE ID : CVE-2020-25022**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.5	An issue was discovered in Noise-Java through 2020-08-27. AESGCMOnCtrCipherState.encryptWithAd() allows out-of-bounds access. **CVE ID : CVE-2020-25023**	https://github.com/rweather/noise-java/pull/12	A-NOI-NOIS-180920/296
octopus					
octopus_deploy					
Information Exposure Through Log Files	09-Sep-20	4.3	In Octopus Deploy 2020.3.x before 2020.3.4 and 2020.4.x before 2020.4.1, if an authenticated user creates a deployment or runbook process using Azure steps and sets the step's execution location to run on the server/worker, then (under certain circumstances) the account password is exposed in cleartext in the verbose task logs output. **CVE ID : CVE-2020-24566**	N/A	A-OCT-OCTO-180920/297
online_bike_rental_project					
online_bike_rental					
Unrestricted Upload of File with Dangerous Type	09-Sep-20	6.5	An Arbitrary File Upload in the Upload Image component in Sourcecodester Online Bike Rental v1.0 allows authenticated administrator to conduct remote code execution. **CVE ID : CVE-2020-24195**	N/A	A-ONL-ONLI-180920/298
openfind					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mail2000					
Incorrect Authorization	01-Sep-20	9	Openfind Mail2000 contains Broken Access Control vulnerability, which can be used to execute unauthorized commands after attackers obtain the administrator access token or cookie. **CVE ID : CVE-2020-12776**	https://www.twcert.org.tw/tw/cp-132-3897-01d73-1.html	A-OPE-MAIL-180920/299
Opensuse					
openldap2					
Acceptance of Extraneous Untrusted Data With Trusted Data	01-Sep-20	7.2	A acceptance of Extraneous Untrusted Data With Trusted Data vulnerability in the start script of openldap2 of SUSE Enterprise Storage 5, SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SECURITY, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud	https://bugzilla.suse.com/show_bug.cgi?id=1172698	A-OPE-OPEN-180920/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to escalate privileges from user ldap to root. This issue affects: SUSE Enterprise Storage 5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Debuginfo 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Debuginfo 11-SP4 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Point of Sale 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 11-SECURITY openldap2-client-openssl1 versions prior to 2.4.26-0.74.13.1. SUSE Linux Enterprise Server 11-SP4-LTSS openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 12-SP2-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP2-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP4 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Server 12-SP5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.31.1. SUSE Linux Enterprise Server for SAP 12-SP2 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 12-SP3 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.31.1. SUSE OpenStack Cloud 7 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud 8 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud Crowbar 8 openldap2 versions prior to 2.4.41-18.71.2. openSUSE Leap 15.1 openldap2 versions prior to 2.4.46-lp151.10.12.1. openSUSE Leap 15.2 openldap2 versions prior to 2.4.46-lp152.14.3.1. **CVE ID : CVE-2020-8023**		
os4ed					
opensis					
Improper Neutralization of Special Elements used in an SQL Command	01-Sep-20	6.5	SQL injection vulnerabilities exist in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The bday parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An	N/A	A-OS4-OPEN-180920/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6117**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerabilities exist in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The bmonth parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6118**	N/A	A-OS4-OPEN-180920/302
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerabilities exist in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The byear parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6119**	N/A	A-OS4-OPEN-180920/303
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerability exists in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The fn parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	N/A	A-OS4-OPEN-180920/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6120		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerabilities exist in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The ln parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6121**	N/A	A-OS4-OPEN-180920/305
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerability exists in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The mn parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6122**	N/A	A-OS4-OPEN-180920/306
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	An exploitable sql injection vulnerability exists in the email parameter functionality of OS4Ed openSIS 7.3. The email parameter in the page EmailCheck.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6123**	N/A	A-OS4-OPEN-180920/307
Improper Neutralization of Special	01-Sep-20	6.5	An exploitable sql injection vulnerability exists in the email parameter functionality of OS4Ed openSIS 7.3. The	N/A	A-OS4-OPEN-180920/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			email parameter in the page EmailCheckOthers.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6124**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	An exploitable SQL injection vulnerability exists in the GetSchool.php functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6125**	N/A	A-OS4-OPEN-180920/309
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerability exists in the CoursePeriodModal.php page of OS4Ed openSIS 7.3. The course_period_id parameter in the page CoursePeriodModal.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger these vulnerabilities. **CVE ID : CVE-2020-6126**	N/A	A-OS4-OPEN-180920/310
Improper Neutralization of Special Elements used in an SQL Command ('SQL	01-Sep-20	6.5	SQL injection vulnerability exists in the CoursePeriodModal.php page of OS4Ed openSIS 7.3. The id parameter in the page CoursePeriodModal.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to	N/A	A-OS4-OPEN-180920/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			trigger this vulnerability. **CVE ID : CVE-2020-6127**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerability exists in the CoursePeriodModal.php page of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. The meet_date parameter in the page CoursePeriodModal.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6128**	N/A	A-OS4-OPEN-180920/312
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerabilities exist in the course_period_id parameters used in OS4Ed openSIS 7.3 pages. The course_period_id parameter in the page CpSessionSet.php is vulnerable to SQL injection.An attacker can make an authenticated HTTP request to trigger these vulnerabilities. **CVE ID : CVE-2020-6129**	N/A	A-OS4-OPEN-180920/313
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerabilities exist in the course_period_id parameters used in OS4Ed openSIS 7.3 pages. The course_period_id parameter in the page MassDropSessionSet.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger these vulnerabilities. **CVE ID : CVE-2020-6130**	N/A	A-OS4-OPEN-180920/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerabilities exist in the course_period_id parameters used in OS4Ed openSIS 7.3 pages. The course_period_id parameter in the page MassScheduleSessionSet.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger these vulnerabilities. **CVE ID : CVE-2020-6131**	N/A	A-OS4-OPEN-180920/315
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerability exists in the ID parameters of OS4Ed openSIS 7.3 pages. The id parameter in the page ChooseCP.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6132**	N/A	A-OS4-OPEN-180920/316
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	SQL injection vulnerabilities exist in the ID parameters of OS4Ed openSIS 7.3 pages. The id parameter in the page CourseMoreInfo.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6133**	N/A	A-OS4-OPEN-180920/317
Improper Neutralization of Special Elements used in an SQL	01-Sep-20	6.5	SQL injection vulnerabilities exist in the ID parameters of OS4Ed openSIS 7.3 pages. The id parameter in the page MassDropModal.php is vulnerable to SQL injection. An attacker can make an	N/A	A-OS4-OPEN-180920/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6134**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	An exploitable SQL injection vulnerability exists in the Validator.php functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6135**	N/A	A-OS4-OPEN-180920/319
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	6.5	An exploitable SQL injection vulnerability exists in the DownloadWindow.php functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6136**	N/A	A-OS4-OPEN-180920/320
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	7.5	SQL injection vulnerability exists in the password reset functionality of OS4Ed openSIS 7.3. The password_stf_email parameter in the password reset page /opensis/ResetUserInfo.php is vulnerable to SQL injection. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6137**	N/A	A-OS4-OPEN-180920/321
Improper Neutralizati	01-Sep-20	7.5	SQL injection vulnerability exists in the password reset	N/A	A-OS4-OPEN-180920/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Special Elements used in an SQL Command ('SQL Injection')			functionality of OS4Ed openSIS 7.3. The uname parameter in the password reset page /opensis/ResetUserInfo.php is vulnerable to SQL injection An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6138**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	7.5	SQL injection vulnerability exists in the password reset functionality of OS4Ed openSIS 7.3. The username_stf_email parameter in the password reset page /opensis/ResetUserInfo.php is vulnerable to SQL injection. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6139**	N/A	A-OS4-OPEN-180920/323
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-20	7.5	SQL injection vulnerability exists in the password reset functionality of OS4Ed openSIS 7.3. The password_stf_email parameter in the password reset page /opensis/ResetUserInfo.php is vulnerable to SQL injection. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6140**	N/A	A-OS4-OPEN-180920/324
Improper Neutralization of Special Elements	01-Sep-20	7.5	An exploitable SQL injection vulnerability exists in the login functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead	N/A	A-OS4-OPEN-180920/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			to SQL injection. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6141**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Sep-20	7.5	A remote code execution vulnerability exists in the Modules.php functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can cause local file inclusion. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6142**	N/A	A-OS4-OPEN-180920/326
Improper Control of Generation of Code ('Code Injection')	01-Sep-20	7.5	A remote code execution vulnerability exists in the install functionality of OS4Ed openSIS 7.4. The password variable which is set at line 122 in install/Step5.php allows for injection of PHP code into the Data.php file that it writes. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6143**	N/A	A-OS4-OPEN-180920/327
Improper Control of Generation of Code ('Code Injection')	01-Sep-20	7.5	A remote code execution vulnerability exists in the install functionality of OS4Ed openSIS 7.4. The username variable which is set at line 121 in install/Step5.php allows for injection of PHP code into the Data.php file that it writes. An attacker can send an HTTP request to trigger this vulnerability.	N/A	A-OS4-OPEN-180920/328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6144		
Oscommerce					
ce_phoenix					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	Several XSS vulnerabilities in osCommerce CE Phoenix before 1.0.6.0 allow an attacker to inject and execute arbitrary JavaScript code. The malicious code can be injected as follows: the page parameter to catalog/admin/order_status.php, catalog/admin/tax_rates.php, catalog/admin/languages.php, catalog/admin/countries.php, catalog/admin/tax_classes.php, catalog/admin/reviews.php, or catalog/admin/zones.php; or the zpage or spage parameter to catalog/admin/geo_zones.php. **CVE ID : CVE-2020-12058**	N/A	A-OSC-CE_P-180920/329
oswapp					
warehouse_inventory_system					
Cross-Site Request Forgery (CSRF)	01-Sep-20	6.8	A Cross-Site Request Forgery (CSRF) vulnerability in edit_user.php in OSWAPP Warehouse Inventory System (aka OSWA-INV) through 2020-08-10 allows remote attackers to change the admin's password after an authenticated admin visits a third-party site. **CVE ID : CVE-2020-23836**	N/A	A-OSW-WARE-180920/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pancakeapp					
pancake					
Use of Hard-coded Credentials	03-Sep-20	5	Use of a hard-coded cryptographic key in Pancake versions < 4.13.29 allows an attacker to forge session cookies, which may lead to remote privilege escalation. **CVE ID : CVE-2020-24876**	N/A	A-PAN-PANC-180920/331
Philips					
patient_information_center_ix					
Exposure of Resource to Wrong Sphere	11-Sep-20	4.6	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product exposes a resource to the wrong control sphere, providing unintended actors with inappropriate access to the resource. The application on the surveillance station operates in kiosk mode, which is vulnerable to local breakouts that could allow an attacker with physical access to escape the restricted environment with limited privileges. **CVE ID : CVE-2020-16212**	N/A	A-PHI-PATI-180920/332
N/A	11-Sep-20	5.8	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue	N/A	A-PHI-PATI-180920/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software saves user-provided information into a comma-separated value (CSV) file, but it does not neutralize or incorrectly neutralizes special elements that could be interpreted as a command when the file is opened by spreadsheet software. **CVE ID : CVE-2020-16214**		
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	A-PHI-PATI-180920/334
Improper Neutralization of Input During Web Page Generation	11-Sep-20	2.7	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-	N/A	A-PHI-PATI-180920/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is then used as a webpage and served to other users. Successful exploitation could lead to unauthorized access to patient data via a read-only web application. **CVE ID : CVE-2020-16218**		
N/A	11-Sep-20	3.3	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input that is expected to be well-formed (i.e., to comply with a certain syntax) but it does not validate or incorrectly validates that the input complies with the syntax, causing the certificate enrollment service to crash. It does not impact monitoring but prevents new devices from enrolling. **CVE ID : CVE-2020-16220**	N/A	A-PHI-PATI-180920/336
Improper Authentication	11-Sep-20	5.8	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue	N/A	A-PHI-PATI-180920/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. When an actor claims to have a given identity, the software does not prove or insufficiently proves the claim is correct. **CVE ID : CVE-2020-16222**		
Improper Handling of Length Parameter Inconsistency	11-Sep-20	3.3	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software parses a formatted message or structure but does not handle or incorrectly handles a length field that is inconsistent with the actual length of the associated data, causing the application on the surveillance station to restart. **CVE ID : CVE-2020-16224**	N/A	A-PHI-PATI-180920/338
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of	N/A	A-PHI-PATI-180920/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**		
performancebridge_focal_point					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	A-PHI-PERF-180920/340
N/A	11-Sep-20	3.3	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input that is expected to be well-formed (i.e., to comply with a certain syntax) but it does not validate or incorrectly validates that the input complies with the syntax, causing the certificate	N/A	A-PHI-PERF-180920/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enrollment service to crash. It does not impact monitoring but prevents new devices from enrolling. **CVE ID : CVE-2020-16220**		
Improper Authentication	11-Sep-20	5.8	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. When an actor claims to have a given identity, the software does not prove or insufficiently proves the claim is correct. **CVE ID : CVE-2020-16222**	N/A	A-PHI-PERF-180920/342
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	A-PHI-PERF-180920/343
PHP					
php					
Improper Input	03-Sep-20	5	An issue was discovered in Chadha PHPKB 9.0 Enterprise	N/A	A-PHP-PHP-180920/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Edition. installer/test-connection.php (part of the installation process) allows a remote unauthenticated attacker to disclose local files on hosts running PHP before 7.2.16, or on hosts where the MySQL ALLOW LOCAL DATA INFILE option is enabled. **CVE ID : CVE-2020-11579**		
Use After Free	09-Sep-20	5.8	In PHP versions 7.2.x below 7.3.21, 7.3.x below 7.3.21 and 7.4.x below 7.4.9, while processing PHAR files using phar extension, phar_parse_zipfile could be tricked into accessing freed memory, which could lead to a crash or information disclosure. **CVE ID : CVE-2020-7068**	https://bugs.php.net/bug.php?id=79797	A-PHP-PHP-180920/345
Php-fusion					
php-fusion					
Improper Privilege Management	03-Sep-20	9	Privilege escalation in PHP-Fusion 9.03.50 downloads/downloads.php allows an authenticated user (not admin) to send a crafted request to the server and perform remote command execution (RCE). **CVE ID : CVE-2020-24949**	N/A	A-PHP-PHP--180920/346
projectworlds					
car_rental_project					
Unrestricted Upload of File with	09-Sep-20	7.5	Arbitrary File Upload in the Vehicle Image Upload component in Project Worlds	N/A	A-PRO-CAR_-180920/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Car Rental Management System v1.0 allows attackers to conduct remote code execution. **CVE ID : CVE-2020-24199**		
Qualcomm					
ips_pdf					
NULL Pointer Dereference	08-Sep-20	7.8	u'Null pointer dereference in HP OfficeJet Pro 8210 jbig2 filter due to lack of check of PDF font array leads to denial of service' in IPS PDF releases prior to IPS System 2020.2 **CVE ID : CVE-2020-11158**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	A-QUA-IPS_-180920/348
raonwiz					
raon_kupload					
Improper Input Validation	02-Sep-20	6.8	RAONWIZ v2018.0.2.50 and earlier versions contains a vulnerability that could allow remote files to be downloaded by lack of validation. Vulnerabilities in downloading with Kupload agent allow files to be downloaded to arbitrary paths due to insufficient verification of extensions and download paths. This issue affects: RAONWIZ RAON KUpload 2018.0.2.50 versions and earlier. **CVE ID : CVE-2020-7830**	N/A	A-RAO-RAON-180920/349
Rapid7					
nexpose					
Improper Control of Generation	03-Sep-20	6.8	In Rapid7 Nexpose installer versions prior to 6.6.40, the Nexpose installer calls an	https://help.rapid7.com/insightvm/en	A-RAP-NEXP-180920/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			executable which can be placed in the appropriate directory by an attacker with access to the local machine. This would prevent the installer from distinguishing between a valid executable called during a Security Console installation and any arbitrary code executable using the same file name. **CVE ID : CVE-2020-7381**	-us/release-notes/index.html?pid=6.6.40	
Unquoted Search Path or Element	03-Sep-20	4.4	Rapid7 Nexpose installer version prior to 6.6.40 contains an Unquoted Search Path which may allow an attacker on the local machine to insert an arbitrary file into the executable path. This issue affects: Rapid7 Nexpose versions prior to 6.6.40. **CVE ID : CVE-2020-7382**	https://help.rapid7.com/insightvm/en-us/release-notes/index.html?pid=6.6.40	A-RAP-NEXP-180920/351
razer					
chroma_sdk					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Sep-20	6.8	Razer Chroma SDK Rest Server through 3.12.17 allows remote attackers to execute arbitrary programs because there is a race condition in which a file created under "%PROGRAMDATA%\Razer Chroma\SDK\Apps" can be replaced before it is executed by the server. The attacker must have access to port 54236 for a registration step. **CVE ID : CVE-2020-16602**	N/A	A-RAZ-CHRO-180920/352
realseriousgames					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
confucious					
Improper Input Validation	01-Sep-20	7.5	All versions of package confucious are vulnerable to Prototype Pollution via the set function. **CVE ID : CVE-2020-7714**	N/A	A-REA-CONF-180920/353
Redhat					
jboss_enterprise_application_platform					
Uncontrolled Resource Consumption	09-Sep-20	5	A flaw was found in JBossWeb in versions before 7.5.31.Final-redhat-3. The fix for CVE-2020-13935 was incomplete in JBossWeb, leaving it vulnerable to a denial of service attack when sending multiple requests with invalid payload length in a WebSocket frame. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-14384**	N/A	A-RED-JBOS-180920/354
jbossweb					
Uncontrolled Resource Consumption	09-Sep-20	5	A flaw was found in JBossWeb in versions before 7.5.31.Final-redhat-3. The fix for CVE-2020-13935 was incomplete in JBossWeb, leaving it vulnerable to a denial of service attack when sending multiple requests with invalid payload length in a WebSocket frame. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-14384**	N/A	A-RED-JBOS-180920/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
safe-object2_project					
safe-object2					
Improper Input Validation	01-Sep-20	7.5	All versions of package safe-object2 are vulnerable to Prototype Pollution via the setter function. **CVE ID : CVE-2020-7726**	N/A	A-SAF-SAFE-180920/356
Samba					
cifs-utils					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Sep-20	4.4	It was found that cifs-utils' mount.cifs was invoking a shell when requesting the Samba password, which could be used to inject arbitrary commands. An attacker able to invoke mount.cifs with special permission, such as via sudo rules, could use this flaw to escalate their privileges. **CVE ID : CVE-2020-14342**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14342	A-SAM-CIFS-180920/357
SAP					
abap_platform					
Improper Control of Generation of Code ('Code Injection')	09-Sep-20	6.5	A Remote Code Execution vulnerability exists in the SAP NetWeaver (ABAP Server, up to release 7.40) and ABAP Platform (> release 7.40).Because of this, an attacker can exploit these products via Code Injection, and potentially enabling to take complete control of the products, including viewing, changing, or deleting data by injecting code into the working memory which is subsequently executed by the	N/A	A-SAP-ABAP-180920/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application. It can also be used to cause a general fault in the product, causing the products to terminate. **CVE ID : CVE-2020-6318**		
netweaver_knowledge_management					
Improper Encoding or Escaping of Output	09-Sep-20	4	SAP NetWeaver Application Server JAVA(XML Forms) versions 7.30, 7.31, 7.40, 7.50 does not sufficiently encode user controlled inputs, which allows an authenticated User with special roles to store malicious content, that when accessed by a victim, can perform malicious actions by executing JavaScript, leading to Stored Cross-Site Scripting. **CVE ID : CVE-2020-6313**	N/A	A-SAP-NETW-180920/359
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-20	3.5	SAP NetWeaver (Knowledge Management), version-7.30,7.31,7.40,7.50, allows an authenticated attacker to create malicious links in the UI, when clicked by victim, will execute arbitrary java scripts thus extracting or modifying information otherwise restricted leading to Stored Cross Site Scripting. **CVE ID : CVE-2020-6326**	N/A	A-SAP-NETW-180920/360
bank_analyzer					
Incorrect Authorization	09-Sep-20	4	Banking services from SAP 9.0 (Bank Analyzer), version - 500, and SAP S/4HANA for financial products subledger, version ? 100, does not correctly perform necessary	N/A	A-SAP-BANK-180920/361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization checks for an authenticated user due to Improper Authorization checks, that may cause a system administrator to create incorrect authorization proposals. This may result in privilege escalation and may expose restricted banking data. **CVE ID : CVE-2020-6311**		
s\/4hana_for_financial_products_subledger					
Incorrect Authorization	09-Sep-20	4	Banking services from SAP 9.0 (Bank Analyzer), version - 500, and SAP S/4HANA for financial products subledger, version ? 100, does not correctly perform necessary authorization checks for an authenticated user due to Improper Authorization checks, that may cause a system administrator to create incorrect authorization proposals. This may result in privilege escalation and may expose restricted banking data. **CVE ID : CVE-2020-6311**	N/A	A-SAP-S\/4-180920/362
3d_visual_enterprise_viewer					
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HPGL file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the	N/A	A-SAP-3D_V-180920/363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6314**		
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated U3D file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6321**	N/A	A-SAP-3D_V-180920/364
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated 3DM file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6322**	N/A	A-SAP-3D_V-180920/365
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated 3DM file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	N/A	A-SAP-3D_V-180920/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6327		
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated CGM file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6328**	N/A	A-SAP-3D_V-180920/367
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated SKP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6329**	N/A	A-SAP-3D_V-180920/368
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated 3DM file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6330**	N/A	A-SAP-3D_V-180920/369
Improper	09-Sep-20	4.3	SAP 3D Visual Enterprise	N/A	A-SAP-3D_V-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Viewer, version - 9, allows a user to open manipulated HPGL file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6331**		180920/370
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HPGL file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6332**	N/A	A-SAP-3D_V-180920/371
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated 3DM file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6333**	N/A	A-SAP-3D_V-180920/372
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated SKP file received from untrusted	N/A	A-SAP-3D_V-180920/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6334**		
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HPGL file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6335**	N/A	A-SAP-3D_V-180920/374
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6336**	N/A	A-SAP-3D_V-180920/375
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HDR file received from untrusted sources which results in crashing of the application and becoming temporarily	N/A	A-SAP-3D_V-180920/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6337**		
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated RH file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6338**	N/A	A-SAP-3D_V-180920/377
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated BMP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6339**	N/A	A-SAP-3D_V-180920/378
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input	N/A	A-SAP-3D_V-180920/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Validation. **CVE ID : CVE-2020-6340**		
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated EPS file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6341**	N/A	A-SAP-3D_V-180920/380
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated U3D file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6342**	N/A	A-SAP-3D_V-180920/381
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated EPS file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6343**	N/A	A-SAP-3D_V-180920/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PDF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6344**	N/A	A-SAP-3D_V-180920/383
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated TGA file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6345**	N/A	A-SAP-3D_V-180920/384
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated BMP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6346**	N/A	A-SAP-3D_V-180920/385
Improper Input	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HDR	N/A	A-SAP-3D_V-180920/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6347**		
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated GIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6348**	N/A	A-SAP-3D_V-180920/387
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated GIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6349**	N/A	A-SAP-3D_V-180920/388
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated BMP file received from untrusted sources which results in crashing of the application and	N/A	A-SAP-3D_V-180920/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6350**		
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated FBX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6351**	N/A	A-SAP-3D_V-180920/390
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated FBX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6352**	N/A	A-SAP-3D_V-180920/391
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated SKP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is	N/A	A-SAP-3D_V-180920/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			caused due to Improper Input Validation. **CVE ID : CVE-2020-6353**		
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated SKP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6354**	N/A	A-SAP-3D_V-180920/393
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated TGA file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6355**	N/A	A-SAP-3D_V-180920/394
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated BMP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	N/A	A-SAP-3D_V-180920/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6356		
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated U3D file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6357**	N/A	A-SAP-3D_V-180920/396
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated FBX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6358**	N/A	A-SAP-3D_V-180920/397
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PLT file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6359**	N/A	A-SAP-3D_V-180920/398
Improper	09-Sep-20	4.3	SAP 3D Visual Enterprise	N/A	A-SAP-3D_V-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Viewer, version - 9, allows a user to open manipulated DIB file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6360**		180920/399
Improper Input Validation	09-Sep-20	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated RLE files received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2020-6361**	N/A	A-SAP-3D_V-180920/400
marketing					
Incorrect Authorization	09-Sep-20	5.5	SAP Marketing (Servlet), version-130,140,150, allows an authenticated attacker to invoke certain functions that are restricted. Limited knowledge of payload is required for an attacker to exploit the vulnerability and perform tasks related to contact and interaction data which impacts Confidentiality and Integrity of data in the application. **CVE ID : CVE-2020-6320**	N/A	A-SAP-MARK-180920/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
commerce					
N/A	09-Sep-20	7.5	SAP Commerce versions 6.7, 1808, 1811, 1905, 2005 contains the jSession ID in the backoffice URL when the application is loaded initially. An attacker can get this session ID via shoulder surfing or man in the middle attack and subsequently get access to admin user accounts, leading to Session Fixation and complete compromise of the confidentiality, integrity and availability of the application. **CVE ID : CVE-2020-6302**	N/A	A-SAP-COMM-180920/402
netweaver_as_abap_business_server_pages					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-20	4.3	SAP Netweaver AS ABAP(BSP Test Application sbspext_table), version-700,701,720,730,731,740,750, 751,752,753,754,755, allows an unauthenticated attacker to send polluted URL to the victim, when the victim clicks on this URL, the attacker can read, modify the information available in the victim?s browser leading to Reflected Cross Site Scripting. **CVE ID : CVE-2020-6324**	N/A	A-SAP-NETW-180920/403
fiori_launchpad					
Improper Neutralization of Input During Web Page Generation	09-Sep-20	4.3	SAP Fiori Launchpad does not sufficiently encode user controlled inputs, and hence allowing the attacker to inject the meta tag into the launchpad html using the	N/A	A-SAP-FIOR-180920/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerable parameter, resulting in reflected Cross-Site Scripting (XSS) vulnerability. With a successful attack, the attacker can steal authentication information of the user, such as data relating to his or her current session. **CVE ID : CVE-2020-6283**		
businessobjects_business_intelligence_platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-20	3.5	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), versions - 4.1, 4.2, allows an attacker with a non-administrative user account that can edit certain web page properties, can modify how a browser processes particular page elements, leading to stored Cross Site Scripting. In certain situations, when a user accesses an affected web page element, the attacker will be able to access or modify metadata for which they are not authorized. **CVE ID : CVE-2020-6312**	N/A	A-SAP-BUSI-180920/405
Unrestricted Upload of File with Dangerous Type	09-Sep-20	5	SAP Business Objects Business Intelligence Platform (Web Intelligence HTML interface) allows an attacker with edit document rights to upload any file (including script files) without proper file format validation leading to Unrestricted upload of file with dangerous type	N/A	A-SAP-BUSI-180920/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. The attacker can modify some formulas and display erroneous content. The server is not affected only the current user browser session, that can easily be closed. **CVE ID : CVE-2020-6288**		
Sensiolabs					
symfony					
Improper Cross-boundary Removal of Sensitive Data	02-Sep-20	7.5	In Symfony before versions 4.4.13 and 5.1.5, the CachingHttpClient class from the HttpClient Symfony component relies on the HttpCache class to handle requests. HttpCache uses internal headers like X-Body-Eval and X-Body-File to control the restoration of cached responses. The class was initially written with surrogate caching and ESI support in mind (all HTTP calls come from a trusted backend in that scenario). But when used by CachingHttpClient and if an attacker can control the response for a request being made by the CachingHttpClient, remote code execution is possible. This has been fixed in versions 4.4.13 and 5.1.5. **CVE ID : CVE-2020-15094**	https://github.com/symfony/symfony/security/advisories/GHSA-754h-5r27-7x3r	A-SEN-SYMF-180920/407
httpclient					
Improper	02-Sep-20	7.5	In Symfony before versions	https://githu	A-SEN-HTTP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-boundary Removal of Sensitive Data			4.4.13 and 5.1.5, the CachingHttpClient class from the HttpClient Symfony component relies on the HttpCache class to handle requests. HttpCache uses internal headers like X-Body-Eval and X-Body-File to control the restoration of cached responses. The class was initially written with surrogate caching and ESI support in mind (all HTTP calls come from a trusted backend in that scenario). But when used by CachingHttpClient and if an attacker can control the response for a request being made by the CachingHttpClient, remote code execution is possible. This has been fixed in versions 4.4.13 and 5.1.5. **CVE ID : CVE-2020-15094**	b.com/symfony/symfony/security/advisories/GHSA-754h-5r27-7x3r	180920/408
senstar					
symphony					
Deserialization of Untrusted Data	01-Sep-20	8.3	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Senstar Symphony 7.3.2.2. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SSOAuth process. The issue results from the lack of proper validation of user-supplied data, which can	N/A	A-SEN-SYMP-180920/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10980. **CVE ID : CVE-2020-17405**		
setelsa-security					
conacwin					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Sep-20	5	** DISPUTED ** Setelsa Conacwin v3.7.1.2 is vulnerable to a local file inclusion vulnerability. This vulnerability allows a remote unauthenticated attacker to read internal files on the server via an http:IP:PORT/../../path/file_to_disclose Directory Traversal URI. NOTE: The manufacturer indicated that the affected version does not exist. CVE-2020-25068 is been disputed until the researcher and the manufacturer identify the correct affected version. **CVE ID : CVE-2020-25068**	N/A	A-SET-CONA-180920/410
shadan-kun					
server_security_type					
Improper Handling of Exceptional Conditions	02-Sep-20	5	Shadankun Server Security Type (excluding normal blocking method types) Ver.1.5.3 and earlier allows remote attackers to cause a denial of service which may result in not being able to add newly detected attack source IP addresses as blocking	N/A	A-SHA-SERV-180920/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			targets for about 10 minutes via a specially crafted request. **CVE ID : CVE-2020-5622**		
Siemens					
simatic_rtls_locating_manager					
Incorrect Default Permissions	09-Sep-20	4.4	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.10.2). The start-stop scripts for the services of the affected application could allow a local attacker to include arbitrary commands that are executed when services are started or stopped interactively by system administrators. **CVE ID : CVE-2020-10049**	N/A	A-SIE-SIMA-180920/412
Incorrect Default Permissions	09-Sep-20	7.2	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.10.2). The directory of service executables of the affected application could allow a local attacker to include arbitrary commands that are executed with SYSTEM privileges when the system restarts. **CVE ID : CVE-2020-10050**	N/A	A-SIE-SIMA-180920/413
Unquoted Search Path or Element	09-Sep-20	7.2	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.10.2). Multiple services of the affected application are executed with SYSTEM privileges while the call path is not quoted. This	N/A	A-SIE-SIMA-180920/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow a local attacker to inject arbitrary commands that are execeuted instead of the legitimate service. **CVE ID : CVE-2020-10051**		
license_management_utility					
Improper Privilege Management	09-Sep-20	7.2	A vulnerability has been identified in License Management Utility (LMU) (All versions < V2.4). The lmgrd service of the affected application is executed with local SYSTEM privileges on the server while its configuration can be modified by local users. The vulnerability could allow a local authenticated attacker to execute arbitrary commands on the server with local SYSTEM privileges. **CVE ID : CVE-2020-10056**	N/A	A-SIE-LICE-180920/415
spectrum_power_4					
Cleartext Storage of Sensitive Information	09-Sep-20	5	A vulnerability has been identified in Spectrum Power 4 (All versions < V4.70 SP8). Insecure storage of sensitive information in the configuration files could allow the retrieval of user names. **CVE ID : CVE-2020-15784**	N/A	A-SIE-SPEC-180920/416
Information Exposure	09-Sep-20	5	A vulnerability has been identified in Spectrum Power 4 (All versions < V4.70 SP8). If configured in an insecure manner, the web server might be susceptible to a directory listing attack.	N/A	A-SIE-SPEC-180920/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15790		
siveillance_video_client					
Cleartext Transmission of Sensitive Information	09-Sep-20	4.3	A vulnerability has been identified in Siveillance Video Client (All versions). In environments where Windows NTLM authentication is enabled the affected client application transmits usernames to the server in cleartext. This could allow an attacker in a privileged network position to obtain valid adminstrator login names and use this information to launch further attacks. **CVE ID : CVE-2020-15785**	N/A	A-SIE-SIVE-180920/418
polarion_subversion_webclient					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-20	4.3	A vulnerability has been identified in Polarion Subversion Webclient (All versions). The Polarion subversion web application does not filter user input in a way that prevents Cross-Site Scripting. If a user is enticed into passing specially crafted, malicious input to the web client (e.g. by clicking on a malicious URL with embedded JavaScript), then JavaScript code can be returned and may then be executed by the user's client. Various actions could be triggered by running malicious JavaScript code. **CVE ID : CVE-2020-15788**	N/A	A-SIE-POLA-180920/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	09-Sep-20	5.8	A vulnerability has been identified in Polarion Subversion Webclient (All versions). The web interface could allow a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link. Successful exploitation requires user interaction by a legitimate user, who must be authenticated to the web interface. A successful attack could allow an attacker to trigger actions via the web interface that the legitimate user is allowed to perform. This could allow the attacker to read or modify contents of the web application. **CVE ID : CVE-2020-15789**	N/A	A-SIE-POLA-180920/420
Spiceworks					
spiceworks					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	Spiceworks Version <= 7.5.00107 is affected by XSS. Any name typed on Custom Groups function is vulnerable to stored XSS as they displayed on http://127.0.0.1/inventory/groups/ without output sanitization. **CVE ID : CVE-2020-23450**	N/A	A-SPI-SPIC-180920/421
Squid-cache					
squid					
Inconsistent	02-Sep-20	3.5	An issue was discovered in Squid before 4.13 and 5.x	N/A	A-SQU-SQUI-180920/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Interpretation of HTTP Requests ('HTTP Request Smuggling')			before 5.0.4. Due to incorrect data validation, HTTP Request Smuggling attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the proxy cache and any downstream caches with content from an arbitrary source. When configured for relaxed header parsing (the default), Squid relays headers containing whitespace characters to upstream servers. When this occurs as a prefix to a Content-Length header, the frame length specified will be ignored by Squid (allowing for a conflicting length to be used from another Content-Length header) but relayed upstream. **CVE ID : CVE-2020-15810**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	02-Sep-20	4	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Splitting attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the browser cache and any downstream caches with content from an arbitrary source. Squid uses a string	N/A	A-SQU-SQUI-180920/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			search instead of parsing the Transfer-Encoding header to find chunked encoding. This allows an attacker to hide a second request inside Transfer-Encoding: it is interpreted by Squid as chunked and split out into a second request delivered upstream. Squid will then deliver two distinct responses to the client, corrupting any downstream caches. **CVE ID : CVE-2020-15811**		
stock_management_system_project					
stock_management_system					
Cross-Site Request Forgery (CSRF)	02-Sep-20	5.8	A Cross-Site Request Forgery (CSRF) vulnerability in changeUsername.php in SourceCodester Stock Management System v1.0 allows remote attackers to deny future logins by changing an authenticated victim's username when they visit a third-party site. **CVE ID : CVE-2020-23830**	N/A	A-STO-STOC-180920/424
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	4.3	A Reflected Cross-Site Scripting (XSS) vulnerability in the index.php login-portal webpage of SourceCodester Stock Management System v1.0 allows remote attackers to harvest login credentials and session cookies when an unauthenticated victim clicks on a malicious URL and enters credentials.	N/A	A-STO-STOC-180920/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-23831		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Sep-20	7.5	A SQL injection vulnerability in the login component in Stock Management System v1.0 allows remote attacker to execute arbitrary SQL commands via the username parameter. **CVE ID : CVE-2020-24197**	N/A	A-STO-STOC-180920/426
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-20	4.3	A persistent cross-site scripting vulnerability in Sourcecodester Stock Management System v1.0 allows remote attackers to inject arbitrary web script or HTML via the 'Brand Name.' **CVE ID : CVE-2020-24198**	N/A	A-STO-STOC-180920/427
superantispyware					
professional_x					
Improper Privilege Management	01-Sep-20	7.2	SUPERAntiSyware Professional X Trial 10.0.1206 is vulnerable to local privilege escalation because it allows unprivileged users to restore a malicious DLL from quarantine into the system32 folder via an NTFS directory junction, as demonstrated by a crafted ualapi.dll file that is detected as malware. **CVE ID : CVE-2020-24955**	N/A	A-SUP-PROF-180920/428
Suse					
linux_enterprise_debuginfo					
Acceptance of	01-Sep-20	7.2	A acceptance of Extraneous Untrusted Data With Trusted	https://bugzilla.suse.com	A-SUS-LINU-180920/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Extraneous Untrusted Data With Trusted Data			Data vulnerability in the start script of openldap2 of SUSE Enterprise Storage 5, SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SECURITY, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to escalate privileges from user ldap to root. This issue affects: SUSE Enterprise Storage 5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Debuginfo 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Debuginfo 11-SP4 openldap2 versions prior to	/show_bug.cgi?id=1172698	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.4.26-0.74.13.1,. SUSE Linux Enterprise Point of Sale 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 11-SECURITY openldap2-client-openssl1 versions prior to 2.4.26-0.74.13.1. SUSE Linux Enterprise Server 11-SP4-LTSS openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 12-SP2-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP2-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP4 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.31.1. SUSE Linux Enterprise Server for SAP 12-SP2 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 12-SP3 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.31.1. SUSE OpenStack		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cloud 7 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud 8 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud Crowbar 8 openldap2 versions prior to 2.4.41-18.71.2. openSUSE Leap 15.1 openldap2 versions prior to 2.4.46-lp151.10.12.1. openSUSE Leap 15.2 openldap2 versions prior to 2.4.46-lp152.14.3.1. **CVE ID : CVE-2020-8023**		
linux_enterprise_point_of_sale					
Acceptance of Extraneous Untrusted Data With Trusted Data	01-Sep-20	7.2	A acceptance of Extraneous Untrusted Data With Trusted Data vulnerability in the start script of openldap2 of SUSE Enterprise Storage 5, SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SECURITY, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise	https://bugzilla.suse.com/show_bug.cgi?id=1172698	A-SUS-LINU-180920/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to escalate privileges from user ldap to root. This issue affects: SUSE Enterprise Storage 5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Debuginfo 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Debuginfo 11-SP4 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Point of Sale 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 11-SECURITY openldap2-client-openssl1 versions prior to 2.4.26-0.74.13.1. SUSE Linux Enterprise Server 11-SP4-LTSS openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 12-SP2-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP2-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Linux Enterprise Server 12-SP4 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.31.1. SUSE Linux Enterprise Server for SAP 12-SP2 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 12-SP3 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.31.1. SUSE OpenStack Cloud 7 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud 8 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud Crowbar 8 openldap2 versions prior to 2.4.41-18.71.2. openSUSE Leap 15.1 openldap2 versions prior to 2.4.46-lp151.10.12.1. openSUSE Leap 15.2 openldap2 versions prior to 2.4.46-lp152.14.3.1. **CVE ID : CVE-2020-8023**		
enterprise_storage					
Acceptance of Extraneous Untrusted Data With Trusted	01-Sep-20	7.2	A acceptance of Extraneous Untrusted Data With Trusted Data vulnerability in the start script of openldap2 of SUSE Enterprise Storage 5, SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise	https://bugzilla.suse.com/show_bug.cgi?id=1172698	A-SUS-ENTE-180920/431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Data			Debuginfo 11-SP4, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SECURITY, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to escalate privileges from user ldap to root. This issue affects: SUSE Enterprise Storage 5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Debuginfo 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Debuginfo 11-SP4 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Point of Sale 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 11-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SECURITY openldap2-client-openssl1 versions prior to 2.4.26-0.74.13.1. SUSE Linux Enterprise Server 11-SP4-LTSS openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 12-SP2-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP2-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP4 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.31.1. SUSE Linux Enterprise Server for SAP 12-SP2 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 12-SP3 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.31.1. SUSE OpenStack Cloud 7 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud 8 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cloud Crowbar 8 openldap2 versions prior to 2.4.41-18.71.2. openSUSE Leap 15.1 openldap2 versions prior to 2.4.46-lp151.10.12.1. openSUSE Leap 15.2 openldap2 versions prior to 2.4.46-lp152.14.3.1. **CVE ID : CVE-2020-8023**		
openstack_cloud					
Acceptance of Extraneous Untrusted Data With Trusted Data	01-Sep-20	7.2	A acceptance of Extraneous Untrusted Data With Trusted Data vulnerability in the start script of openldap2 of SUSE Enterprise Storage 5, SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SECURITY, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud	https://bugzilla.suse.com/show_bug.cgi?id=1172698	A-SUS-OPEN-180920/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Crowbar 8; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to escalate privileges from user ldap to root. This issue affects: SUSE Enterprise Storage 5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Debuginfo 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Debuginfo 11-SP4 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Point of Sale 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 11-SECURITY openldap2-client-openssl1 versions prior to 2.4.26-0.74.13.1. SUSE Linux Enterprise Server 11-SP4-LTSS openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 12-SP2-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP2-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP4 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP5 openldap2 versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.4.41-18.71.2. SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.31.1. SUSE Linux Enterprise Server for SAP 12-SP2 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 12-SP3 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.31.1. SUSE OpenStack Cloud 7 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud 8 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud Crowbar 8 openldap2 versions prior to 2.4.41-18.71.2. openSUSE Leap 15.1 openldap2 versions prior to 2.4.46-lp151.10.12.1. openSUSE Leap 15.2 openldap2 versions prior to 2.4.46-lp152.14.3.1. **CVE ID : CVE-2020-8023**		
openstack_cloud_crowbar					
Acceptance of Extraneous Untrusted Data With Trusted Data	01-Sep-20	7.2	A acceptance of Extraneous Untrusted Data With Trusted Data vulnerability in the start script of openldap2 of SUSE Enterprise Storage 5, SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SECURITY, SUSE Linux Enterprise Server 11-	https://bugzilla.suse.com/show_bug.cgi?id=1172698	A-SUS-OPEN-180920/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SP4-LTSS, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to escalate privileges from user ldap to root. This issue affects: SUSE Enterprise Storage 5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Debuginfo 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Debuginfo 11-SP4 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Point of Sale 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 11-SECURITY openldap2-client-openssl1 versions prior to 2.4.26-0.74.13.1. SUSE Linux Enterprise Server 11-SP4-LTSS openldap2 versions prior		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 12-SP2-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP2-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP4 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.31.1. SUSE Linux Enterprise Server for SAP 12-SP2 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 12-SP3 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.31.1. SUSE OpenStack Cloud 7 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud 8 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud Crowbar 8 openldap2 versions prior to 2.4.41-18.71.2. openSUSE Leap 15.1 openldap2 versions prior to 2.4.46-lp151.10.12.1.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			openSUSE Leap 15.2 openldap2 versions prior to 2.4.46-lp152.14.3.1. **CVE ID : CVE-2020-8023**		
tailor_management_system_project					
tailor_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	4.3	A Reflected Cross-Site Scripting (XSS) vulnerability in the index.php login-portal webpage of SourceCodester Tailor Management System v1.0 allows remote attackers to harvest keys pressed by an unauthenticated victim who clicks on a malicious URL and begins typing. **CVE ID : CVE-2020-23835**	N/A	A-TAI-TAIL-180920/434
taoensso					
nippy					
Deserialization of Untrusted Data	11-Sep-20	6.8	A deserialization flaw is present in Taoensso Nippy before 2.14.2. In some circumstances, it is possible for an attacker to create a malicious payload that, when deserialized, will allow arbitrary code to be executed. This occurs because there is automatic use of the Java Serializable interface. **CVE ID : CVE-2020-24164**	N/A	A-TAO-NIPP-180920/435
teamwire					
teamwire					
Incorrect Authorization	02-Sep-20	3.6	The Teamwire application 5.3.0 for Android allows physically proximate attackers to exploit a flaw related to the	N/A	A-TEA-TEAM-180920/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pass-code component. **CVE ID : CVE-2020-12621**		
Tencent					
tim					
Untrusted Search Path	03-Sep-20	4.4	Shenzhen Tencent TIM Windows client 3.0.0.21315 has a DLL hijacking vulnerability, which can be exploited by attackers to execute malicious code. **CVE ID : CVE-2020-24160**	N/A	A-TEN-TIM-180920/437
tencent					
Uncontrolled Search Path Element	03-Sep-20	4.4	The Shenzhen Tencent app 5.8.2.5300 for PC platforms (from Tencent App Center) has a DLL hijacking vulnerability. Attackers can use this vulnerability to execute malicious code. **CVE ID : CVE-2020-24162**	N/A	A-TEN-TENC-180920/438
tiny-conf_project					
tiny-conf					
Improper Input Validation	01-Sep-20	7.5	All versions of package tiny-conf are vulnerable to Prototype Pollution via the set function. **CVE ID : CVE-2020-7724**	N/A	A-TIN-TINY-180920/439
tradingtechnologies					
trading_technologies_messaging					
Improper Input Validation	02-Sep-20	5	A flaw exists in Trading Technologies Messaging 7.1.28.3 (ttmd.exe) due to improper validation of user-supplied data when processing a type 8 message sent to default TCP	N/A	A-TRA-TRAD-180920/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RequestPort 10200. An unauthenticated, remote attacker can exploit this issue, via a specially crafted message, to terminate ttmd.exe. **CVE ID : CVE-2020-5778**		
N/A	02-Sep-20	5	A flaw in Trading Technologies Messaging 7.1.28.3 (ttmd.exe) relates to invalid parameter handling when calling strcpy_s() with an invalid parameter (i.e., a long src string parameter) as a part of processing a type 4 message sent to default TCP RequestPort 10200. It's been observed that ttmd.exe terminates as a result. **CVE ID : CVE-2020-5779**	N/A	A-TRA-TRAD-180920/441
Trendmicro					
apex_one					
Improper Privilege Management	01-Sep-20	7.2	A vulnerability in Trend Micro Apex One and OfficeScan XG SP1 on Microsoft Windows may allow an attacker to create a hard link to any file on the system, which then could be manipulated to gain a privilege escalation and code execution. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but	N/A	A-TRE-APEX-180920/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			previous versions are affected. **CVE ID : CVE-2020-24556**		
Improper Privilege Management	01-Sep-20	7.2	A vulnerability in Trend Micro Apex One on Microsoft Windows may allow an attacker to manipulate a particular product folder to disable the security temporarily, abuse a specific Windows function and attain privilege escalation. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected. **CVE ID : CVE-2020-24557**	N/A	A-TRE-APEX-180920/443
Out-of-bounds Read	01-Sep-20	3.6	A vulnerability in an Trend Micro Apex One dll may allow an attacker to manipulate it to cause an out-of-bounds read that crashes multiple processes in the product. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2020-24558**	N/A	A-TRE-APEX-180920/444
Improper Privilege Management	01-Sep-20	7.2	A vulnerability in Trend Micro Apex One on macOS may allow an attacker to manipulate a certain binary to load and run a script from a user-writable	N/A	A-TRE-APEX-180920/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			folder, which then would allow them to execute arbitrary code as root. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2020-24559**		
ucms_project					
ucms					
Incorrect Authorization	04-Sep-20	5	An Incorrect Access Control vulnerability exists in /ucms/chk.php in UCMS 1.4.8. This results in information leak via an error message caused by directly accessing the website built by UCMS. **CVE ID : CVE-2020-24981**	N/A	A-UCM-UCMS-180920/446
u-root					
u-root					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Sep-20	5	This affects all versions of package github.com/u-root/u-root/pkg/uzip. It is vulnerable to both leading and non-leading relative path traversal attacks in zip file extraction. **CVE ID : CVE-2020-7665**	N/A	A-U-R-U-RO-180920/447
Improper Limitation of a Pathname to a Restricted Directory ('Path	01-Sep-20	5	This affects all versions of package github.com/u-root/u-root/pkg/cpio. It is vulnerable to leading, non-leading relative path traversal attacks and symlink based (relative and absolute) path traversal	https://github.com/u-root/u-root/pull/1817, https://snyk.io/vuln/SNYK-GOLANG-	A-U-R-U-RO-180920/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			attacks in cpio file extraction. **CVE ID : CVE-2020-7666**	GITHUBCOMUROOTUROOTPKGCPIO-570440	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Sep-20	5	This affects all versions of package github.com/u-root/u-root/pkg/tarutil. It is vulnerable to both leading and non-leading relative path traversal attacks in tar file extraction. **CVE ID : CVE-2020-7669**	https://github.com/u-root/u-root/pull/1817, https://snyk.io/vuln/SNYK-GOLANG-GITHUBCOMUROOTUROOTPKGTARUTIL-570428	A-U-R-U-RO-180920/449
Usvn					
usvn					
N/A	01-Sep-20	7.5	USVN (aka User-friendly SVN) before 1.0.10 allows attackers to execute arbitrary code in the commit view. **CVE ID : CVE-2020-25069**	N/A	A-USV-USVN-180920/450
Cross-Site Request Forgery (CSRF)	01-Sep-20	6.8	USVN (aka User-friendly SVN) before 1.0.10 allows CSRF, related to the lack of the SameSite Strict feature. **CVE ID : CVE-2020-25070**	N/A	A-USV-USVN-180920/451
Vbulletin					
vbulletin					
Improper Neutralization of Input During Web Page Generation ('Cross-site	03-Sep-20	3.5	The Admin CP in vBulletin 5.6.3 allows XSS via an Occupation Title or Description to User Profile Field Manager. **CVE ID : CVE-2020-25115**	N/A	A-VBU-VBUL-180920/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	3.5	The Admin CP in vBulletin 5.6.3 allows XSS via an Announcement Title to Channel Manager. **CVE ID : CVE-2020-25116**	N/A	A-VBU-VBUL-180920/453
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	3.5	The Admin CP in vBulletin 5.6.3 allows XSS via a Junior Member Title to User Title Manager. **CVE ID : CVE-2020-25117**	N/A	A-VBU-VBUL-180920/454
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	3.5	The Admin CP in vBulletin 5.6.3 allows XSS via a Style Options Settings Title to Styles Manager. **CVE ID : CVE-2020-25118**	N/A	A-VBU-VBUL-180920/455
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	3.5	The Admin CP in vBulletin 5.6.3 allows XSS via a Title of a Child Help Item in the Login/Logoff part of the User Manual. **CVE ID : CVE-2020-25119**	N/A	A-VBU-VBUL-180920/456
Improper Neutralization of Input During Web Page Generation	03-Sep-20	3.5	The Admin CP in vBulletin 5.6.3 allows XSS via the admincp/search.php?do=dosearch URI. **CVE ID : CVE-2020-25120**	N/A	A-VBU-VBUL-180920/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	3.5	The Admin CP in vBulletin 5.6.3 allows XSS via the Paid Subscription Email Notification field in the Options. **CVE ID : CVE-2020-25121**	N/A	A-VBU-VBUL-180920/458
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	3.5	The Admin CP in vBulletin 5.6.3 allows XSS via a Rank Type to User Rank Manager. **CVE ID : CVE-2020-25122**	N/A	A-VBU-VBUL-180920/459
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	3.5	The Admin CP in vBulletin 5.6.3 allows XSS via a Smilie Title to Smilies Manager. **CVE ID : CVE-2020-25123**	N/A	A-VBU-VBUL-180920/460
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	3.5	The Admin CP in vBulletin 5.6.3 allows XSS via an admincp/attachment.php&do=rebuild&type= URI. **CVE ID : CVE-2020-25124**	N/A	A-VBU-VBUL-180920/461
webdesi9					
file_manager					
Unrestricted Upload of	09-Sep-20	7.5	The File Manager (wp-file-manager) plugin before 6.9 for	N/A	A-WEB-FILE-180920/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			WordPress allows remote attackers to upload and execute arbitrary PHP code because it renames an unsafe example elFinder connector file to have the .php extension. This, for example, allows attackers to run the elFinder upload (or mkfile and put) command to write PHP code into the wp-content/plugins/wp-file-manager/lib/files/ directory. This was exploited in the wild in August and September 2020. **CVE ID : CVE-2020-25213**		
whatsapp					
whatsapp					
Out-of-bounds Write	03-Sep-20	6.8	A buffer overflow in WhatsApp for Android prior to v2.20.11 and WhatsApp Business for Android prior to v2.20.2 could have allowed an out-of-bounds write via a specially crafted video stream after receiving and answering a malicious video call. **CVE ID : CVE-2020-1886**	https://www.whatsapp.com/security/advisories/2020	A-WHA-WHAT-180920/463
Improper Input Validation	03-Sep-20	5	A URL validation issue in WhatsApp for Android prior to v2.20.11 and WhatsApp Business for Android prior to v2.20.2 could have caused the recipient of a sticker message containing deliberately malformed data to load an image from a sender-controlled URL without user	https://www.whatsapp.com/security/advisories/2020	A-WHA-WHAT-180920/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction. **CVE ID : CVE-2020-1890**		
Out-of-bounds Write	03-Sep-20	7.5	A user controlled parameter used in video call in WhatsApp for Android prior to v2.20.17, WhatsApp Business for Android prior to v2.20.7, WhatsApp for iPhone prior to v2.20.20, and WhatsApp Business for iPhone prior to v2.20.20 could have allowed an out-of-bounds write on 32-bit devices. **CVE ID : CVE-2020-1891**	https://www.whatsapp.com/security/advisories/2020	A-WHA-WHAT-180920/465
Out-of-bounds Write	03-Sep-20	6.8	A stack write overflow in WhatsApp for Android prior to v2.20.35, WhatsApp Business for Android prior to v2.20.20, WhatsApp for iPhone prior to v2.20.30, and WhatsApp Business for iPhone prior to v2.20.30 could have allowed arbitrary code execution when playing a specially crafted push to talk message. **CVE ID : CVE-2020-1894**	https://www.whatsapp.com/security/advisories/2020	A-WHA-WHAT-180920/466
whatsapp_desktop					
Improper Privilege Management	03-Sep-20	7.5	A security feature bypass issue in WhatsApp Desktop versions prior to v0.3.4932 could have allowed for sandbox escape in Electron and escalation of privilege if combined with a remote code execution vulnerability inside the sandboxed renderer process. **CVE ID : CVE-2020-1889**	https://www.whatsapp.com/security/advisories/2020/	A-WHA-WHAT-180920/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
whatsapp_business					
Out-of-bounds Write	03-Sep-20	6.8	A buffer overflow in WhatsApp for Android prior to v2.20.11 and WhatsApp Business for Android prior to v2.20.2 could have allowed an out-of-bounds write via a specially crafted video stream after receiving and answering a malicious video call. **CVE ID : CVE-2020-1886**	https://www.whatsapp.com/security/advisories/2020	A-WHA-WHAT-180920/468
Improper Input Validation	03-Sep-20	5	A URL validation issue in WhatsApp for Android prior to v2.20.11 and WhatsApp Business for Android prior to v2.20.2 could have caused the recipient of a sticker message containing deliberately malformed data to load an image from a sender-controlled URL without user interaction. **CVE ID : CVE-2020-1890**	https://www.whatsapp.com/security/advisories/2020	A-WHA-WHAT-180920/469
Out-of-bounds Write	03-Sep-20	7.5	A user controlled parameter used in video call in WhatsApp for Android prior to v2.20.17, WhatsApp Business for Android prior to v2.20.7, WhatsApp for iPhone prior to v2.20.20, and WhatsApp Business for iPhone prior to v2.20.20 could have allowed an out-of-bounds write on 32-bit devices. **CVE ID : CVE-2020-1891**	https://www.whatsapp.com/security/advisories/2020	A-WHA-WHAT-180920/470
Out-of-bounds Write	03-Sep-20	6.8	A stack write overflow in WhatsApp for Android prior to v2.20.35, WhatsApp Business	https://www.whatsapp.com/security	A-WHA-WHAT-180920/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Android prior to v2.20.20, WhatsApp for iPhone prior to v2.20.30, and WhatsApp Business for iPhone prior to v2.20.30 could have allowed arbitrary code execution when playing a specially crafted push to talk message. **CVE ID : CVE-2020-1894**	/advisories/2020	
X.org					
xorg-server					
Integer Overflow or Wraparound	15-Sep-20	4.6	A flaw was found in xorg-x11-server before 1.20.9. An integer underflow in the X input extension protocol decoding in the X server may lead to arbitrary access of memory contents. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-14346**	N/A	A-X.O-XORG-180920/472
Integer Overflow or Wraparound	15-Sep-20	4.6	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Integer underflow leading to heap-buffer overflow may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-14361**	N/A	A-X.O-XORG-180920/473
Integer Overflow or Wraparoun	15-Sep-20	4.6	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Integer underflow	N/A	A-X.O-XORG-180920/474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d			leading to heap-buffer overflow may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-14362**		
Xmlsoft					
libxml2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Sep-20	7.5	GNOME project libxml2 v2.9.10 and earlier have a global buffer over-read vulnerability in xmlEncodeEntitiesInternal at libxml2/entities.c. The issue has been fixed in commit 8e7c20a1 (20910-GITv2.9.10-103-g8e7c20a1). **CVE ID : CVE-2020-24977**	N/A	A-XML-LIBX-180920/475
xpdfreader					
xpdf					
Improper Initialization	03-Sep-20	6.8	There is an invalid memory access in the function TextString::~TextString() located in Catalog.cc in Xpdf 4.0.2. It can be triggered by (for example) sending a crafted pdf file to the pdftohtml binary, which allows a remote attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact. **CVE ID : CVE-2020-24996**	N/A	A-XPD-XPDF-180920/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Sep-20	6.8	There is an invalid memory access in the function fprintf located in Error.cc in Xpdf 4.0.2. It can be triggered by sending a crafted PDF file to the pdftohtml binary, which allows a remote attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact. **CVE ID : CVE-2020-24999**	N/A	A-XPD-XPDF-180920/477
xuxueli					
xxl-job					
Information Exposure	03-Sep-20	5	xxl-job 2.2.0 allows Information Disclosure of username, model, and password via job/admin/controller/UserController.java. **CVE ID : CVE-2020-23811**	N/A	A-XUX-XXL--180920/478
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-20	4.3	Multiple cross-site scripting (XSS) vulnerabilities in xxl-job v2.2.0 allow remote attackers to inject arbitrary web script or HTML via (1) AppName and (2)AddressList parameter in JobGroupController.java file. **CVE ID : CVE-2020-23814**	N/A	A-XUX-XXL--180920/479
Xwiki					
Xwiki					
Improper Control of Generation of Code ('Code Injection')	10-Sep-20	6	In XWiki before versions 11.10.5 or 12.2.1, any user with SCRIPT right (EDIT right before XWiki 7.4) can gain access to the application server Servlet context which	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-	A-XWI-XWIK-180920/480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contains tools allowing to instantiate arbitrary Java objects and invoke methods that may lead to arbitrary code execution. The only workaround is to give SCRIPT right only to trusted users. **CVE ID : CVE-2020-15171**	7qw5-pqhc-xm4g	
Yaws					
Yaws					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Sep-20	10	CGI implementation in Yaws web server versions 1.81 to 2.0.7 is vulnerable to OS command injection. **CVE ID : CVE-2020-24916**	N/A	A-YAW-YAWS-180920/481
Yodobashi					
Yodobashi					
URL Redirection to Untrusted Site ('Open Redirect')	09-Sep-20	5.8	Yodobashi App for Android versions 1.8.7 and earlier allows remote attackers to lead a user to access an arbitrary website via the vulnerable App. As a result, the user may become a victim of a phishing attack. **CVE ID : CVE-2020-5627**	N/A	A-YOD-YODO-180920/482
yola					
promisehelpers					
Improper Input Validation	01-Sep-20	7.5	All versions of package promisehelpers are vulnerable to Prototype Pollution via the	N/A	A-YOL-PROM-180920/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insert function. **CVE ID : CVE-2020-7723**		
zulipchat					
zulip_desktop					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	4.3	Zulip Desktop before 5.4.3 allows XSS because string escaping is mishandled during composition of the HTML for the user interface. **CVE ID : CVE-2020-24582**	https://blog.zulip.com/2020/09/10/zulip-desktop-5-4-3-security-release/	A-ZUL-ZULI-180920/484
Operating System					
Apple					
mac_os					
Out-of-bounds Read	01-Sep-20	3.6	A vulnerability in an Trend Micro Apex One dll may allow an attacker to manipulate it to cause an out-of-bounds read that crashes multiple processes in the product. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2020-24558**	N/A	O-APP-MAC_-180920/485
Improper Privilege Management	01-Sep-20	7.2	A vulnerability in Trend Micro Apex One on macOS may allow an attacker to manipulate a certain binary to load and run a script from a user-writable folder, which then would allow them to execute arbitrary code as root. An attacker must first obtain the ability to execute low-	N/A	O-APP-MAC_-180920/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2020-24559**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	6.8	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user. **CVE ID : CVE-2020-9727**	N/A	O-APP-MAC_-180920/487
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	6.8	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user. **CVE ID : CVE-2020-9728**	N/A	O-APP-MAC_-180920/488
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	6.8	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user. **CVE ID : CVE-2020-9729**	N/A	O-APP-MAC_-180920/489
Improper	10-Sep-20	6.8	A memory corruption	N/A	O-APP-MAC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user. **CVE ID : CVE-2020-9730**		180920/490
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-20	6.8	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user. **CVE ID : CVE-2020-9731**	N/A	O-APP-MAC_-180920/491
Canonical					
ubuntu_linux					
Information Exposure	01-Sep-20	2.1	The modprobe child process in the ./debian/patches/load_ppp_generic_if_needed patch file incorrectly handled module loading. A local non-root attacker could exploit the MODPROBE_OPTIONS environment variable to read arbitrary root files. Fixed in 2.4.5-5ubuntu1.4, 2.4.5-5.1ubuntu2.3+esm2, 2.4.7-1+2ubuntu1.16.04.3, 2.4.7-2+2ubuntu1.3, 2.4.7-2+4.1ubuntu5.1, 2.4.7-2+4.1ubuntu6. Was ZDI-CAN-	N/A	O-CAN-UBUN-180920/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11504. **CVE ID : CVE-2020-15704**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	02-Sep-20	3.5	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Smuggling attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the proxy cache and any downstream caches with content from an arbitrary source. When configured for relaxed header parsing (the default), Squid relays headers containing whitespace characters to upstream servers. When this occurs as a prefix to a Content-Length header, the frame length specified will be ignored by Squid (allowing for a conflicting length to be used from another Content-Length header) but relayed upstream. **CVE ID : CVE-2020-15810**	N/A	O-CAN-UBUN-180920/493
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	02-Sep-20	4	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Splitting attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local	N/A	O-CAN-UBUN-180920/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security and poison the browser cache and any downstream caches with content from an arbitrary source. Squid uses a string search instead of parsing the Transfer-Encoding header to find chunked encoding. This allows an attacker to hide a second request inside Transfer-Encoding: it is interpreted by Squid as chunked and split out into a second request delivered upstream. Squid will then deliver two distinct responses to the client, corrupting any downstream caches. **CVE ID : CVE-2020-15811**		
Incorrect Default Permissions	01-Sep-20	5	An issue was discovered in Django 2.2 before 2.2.16, 3.0 before 3.0.10, and 3.1 before 3.1.1 (when Python 3.7+ is used). FILE_UPLOAD_DIRECTORY_PERMISSIONS mode was not applied to intermediate-level directories created in the process of uploading files. It was also not applied to intermediate-level collected static directories when using the collectstatic management command. **CVE ID : CVE-2020-24583**	N/A	O-CAN-UBUN-180920/495
Incorrect Default Permissions	01-Sep-20	5	An issue was discovered in Django 2.2 before 2.2.16, 3.0 before 3.0.10, and 3.1 before 3.1.1 (when Python 3.7+ is	N/A	O-CAN-UBUN-180920/496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used). The intermediate-level directories of the filesystem cache had the system's standard umask rather than 0o077. **CVE ID : CVE-2020-24584**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Sep-20	4.3	In KDE Ark before 20.08.1, a crafted TAR archive with symlinks can install files outside the extraction directory, as demonstrated by a write operation to a user's home directory. **CVE ID : CVE-2020-24654**	https://bugzilla.suse.com/show_bug.cgi?id=1175857, https://github.com/KDE/ark/commit/8bf8c5ef07b0ac5e914d752681e470dea403a5bd, https://kde.org/info/security/advisory-20200827-1.txt	O-CAN-UBUN-180920/497
Cisco					
asyncos					
Improper Input Validation	04-Sep-20	5	A vulnerability in the web-based management interface of Cisco AsyncOS software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to insufficient validation of requests that are sent to the web-based management interface. An attacker could exploit this vulnerability by	N/A	O-CIS-ASYN-180920/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to the interface of an affected device. A successful exploit could allow the attacker to obtain the IP addresses that are configured on the internal interfaces of the affected device. There is a workaround that addresses this vulnerability. **CVE ID : CVE-2020-3546**		
fxos					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.2	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could exploit this vulnerability by supplying a crafted file that, when it is processed, may cause a stack-based buffer overflow. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An attacker would need to have valid administrative credentials to exploit this vulnerability. **CVE ID : CVE-2020-3545**	N/A	O-CIS-FXOS-180920/499
rv340w_firmware					
Improper Restriction	04-Sep-20	6.5	Multiple vulnerabilities in the web-based management	N/A	O-CIS-RV34-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3451**		180920/500
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.7	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3453**	N/A	O-CIS-RV34-180920/501
rv340_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system	N/A	O-CIS-RV34-180920/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3451**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.7	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3453**	N/A	O-CIS-RV34-180920/503
rv345_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3451**	N/A	O-CIS-RV34-180920/504
Improper Restriction	04-Sep-20	7.7	Multiple vulnerabilities in the web-based management	N/A	O-CIS-RV34-180920/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3453**		
rv345p_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3451**	N/A	O-CIS-RV34-180920/506
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.7	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system	N/A	O-CIS-RV34-180920/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3453**		
ios_xr					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**	N/A	O-CIS-IOS_-180920/508
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid	N/A	O-CIS-IOS_-180920/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
Debian					
debian_linux					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	02-Sep-20	3.5	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Smuggling attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the proxy cache and any downstream caches with content from an arbitrary source. When configured for relaxed header parsing (the default), Squid relays headers containing	N/A	O-DEB-DEBI-180920/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			whitespace characters to upstream servers. When this occurs as a prefix to a Content-Length header, the frame length specified will be ignored by Squid (allowing for a conflicting length to be used from another Content-Length header) but relayed upstream. **CVE ID : CVE-2020-15810**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	02-Sep-20	4	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Splitting attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the browser cache and any downstream caches with content from an arbitrary source. Squid uses a string search instead of parsing the Transfer-Encoding header to find chunked encoding. This allows an attacker to hide a second request inside Transfer-Encoding: it is interpreted by Squid as chunked and split out into a second request delivered upstream. Squid will then deliver two distinct responses to the client, corrupting any downstream caches. **CVE ID : CVE-2020-15811**	N/A	O-DEB-DEBI-180920/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Sep-20	4.3	In KDE Ark before 20.08.1, a crafted TAR archive with symlinks can install files outside the extraction directory, as demonstrated by a write operation to a user's home directory. **CVE ID : CVE-2020-24654**	https://bugzilla.suse.com/show_bug.cgi?id=1175857, https://github.com/KDE/ark/commit/8bf8c5ef07b0ac5e914d752681e470dea403a5bd, https://kde.org/info/security/advisory-20200827-1.txt	O-DEB-DEBI-180920/512
Out-of-bounds Write	09-Sep-20	5	url::recvline in url.cpp in libproxy 0.4.x through 0.4.15 allows a remote HTTP server to trigger uncontrolled recursion via a response composed of an infinite stream that lacks a newline character. This leads to stack exhaustion. **CVE ID : CVE-2020-25219**	N/A	O-DEB-DEBI-180920/513
N/A	03-Sep-20	4.6	The package grunt before 1.3.0 are vulnerable to Arbitrary Code Execution due to the default usage of the function load() instead of its secure replacement safeLoad() of the package js-yaml inside grunt.file.readYAML. **CVE ID : CVE-2020-7729**	https://github.com/gruntjs/grunt/blob/master/lib/grunt/file.js%23L249, https://github.com/gruntjs/grunt/commit/e350cea1724eb3476464561a380fb6a64e61e4	O-DEB-DEBI-180920/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				e7, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-607922, https://snyk.io/vuln/SNYK-JS-GRUNT-597546	
Dell					
emc_powerscale_onefs					
Incorrect Permission Assignment for Critical Resource	02-Sep-20	6.5	Dell EMC Isilon OneFS versions 8.2.2 and earlier and Dell EMC PowerScale OneFS version 9.0.0 contain a privilege escalation vulnerability. An authenticated malicious user may exploit this vulnerability by using SyncIQ to gain unauthorized access to system management files. **CVE ID : CVE-2020-5369**	N/A	O-DEL-EMC_-180920/515
inspiron_7347_bios					
Use After Free	02-Sep-20	7.2	Dell Inspiron 7347 BIOS versions prior to A13 contain a UEFI BIOS Boot Services overwrite vulnerability. A local attacker with access to system memory may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in System Management Mode (SMM).	N/A	O-DEL-INSP-180920/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5376		
g7_17_7790_bios					
Use After Free	02-Sep-20	7.2	Dell G7 17 7790 BIOS versions prior to 1.13.2 contain a UEFI BIOS Boot Services overwrite vulnerability. A local attacker with access to system memory may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in System Management Mode (SMM). **CVE ID : CVE-2020-5378**	N/A	O-DEL-G7_1-180920/517
inspiron_7352_bios					
N/A	02-Sep-20	7.2	Dell Inspiron 7352 BIOS versions prior to A12 contain a UEFI BIOS Boot Services overwrite vulnerability. A local attacker with access to system memory may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in System Management Mode (SMM). **CVE ID : CVE-2020-5379**	N/A	O-DEL-INSP-180920/518
Dlink					
dcs-2530l_firmware					
N/A	02-Sep-20	9	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. cgi-bin/ddns_enc.cgi allows authenticated command injection.	N/A	O-DLI-DCS--180920/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-25079		
dcs-2670l_firmware					
N/A	02-Sep-20	9	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. cgi-bin/ddns_enc.cgi allows authenticated command injection. **CVE ID : CVE-2020-25079**	N/A	O-DLI-DCS--180920/520
D-link					
dcs-2530l_firmware					
N/A	02-Sep-20	5	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. The unauthenticated /config/getuser endpoint allows for remote administrator password disclosure. **CVE ID : CVE-2020-25078**	N/A	O-D-L-DCS--180920/521
dcs-2670l_firmware					
N/A	02-Sep-20	5	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. The unauthenticated /config/getuser endpoint allows for remote administrator password disclosure. **CVE ID : CVE-2020-25078**	N/A	O-D-L-DCS--180920/522
Fedoraproject					
fedora					
Inconsisten	02-Sep-20	4	An issue was discovered in	N/A	O-FED-FEDO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t Interpretation of HTTP Requests ('HTTP Request Smuggling')			Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Splitting attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the browser cache and any downstream caches with content from an arbitrary source. Squid uses a string search instead of parsing the Transfer-Encoding header to find chunked encoding. This allows an attacker to hide a second request inside Transfer-Encoding: it is interpreted by Squid as chunked and split out into a second request delivered upstream. Squid will then deliver two distinct responses to the client, corrupting any downstream caches. **CVE ID : CVE-2020-15811**		180920/523
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Sep-20	4.3	In KDE Ark before 20.08.1, a crafted TAR archive with symlinks can install files outside the extraction directory, as demonstrated by a write operation to a user's home directory. **CVE ID : CVE-2020-24654**	https://bugzilla.suse.com/show_bug.cgi?id=1175857, https://github.com/KDE/ark/commit/8bf8c5ef07b0ac5e914d752681e470dea403a5bd,	O-FED-FEDO-180920/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://kde.org/info/security/advisory-20200827-1.txt	
Out-of-bounds Write	04-Sep-20	5	An issue was discovered in GnuTLS before 3.6.15. A server can trigger a NULL pointer dereference in a TLS 1.3 client if a no_renegotiation alert is sent with unexpected timing, and then an invalid second handshake occurs. The crash happens in the application's error handling path, where the gnutls_deinit function is called after detecting a handshake failure. **CVE ID : CVE-2020-24659**	https://security.netapp.com/advisory/ntap-20200911-0006/	O-FED-FEDO-180920/525
Freebsd					
freebsd					
NULL Pointer Dereference	03-Sep-20	4.9	In MidnightBSD before 1.2.6 and 1.3 before August 2020, and FreeBSD before 7, a NULL pointer dereference was found in the Linux emulation layer that allows attackers to crash the running kernel. During binary interaction, td->td_emuldata in sys/compat/linux/linux_emul.h is not getting initialized and returns NULL from em_find(). **CVE ID : CVE-2020-24385**	http://www.midnightbsd.org/security/adv/MIDNIGHTBSD-SA-20:02.txt	O-FRE-FREE-180920/526
Out-of-bounds Write	03-Sep-20	4.9	A memory corruption vulnerability was found in the kernel function kern_getfsstat in MidnightBSD before 1.2.7	http://www.midnightbsd.org/security/adv/MIDNI	O-FRE-FREE-180920/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 1.3 through 2020-08-19, and FreeBSD through 11.4, that allows an attacker to trigger an invalid free and crash the system via a crafted size value in conjunction with an invalid mode. **CVE ID : CVE-2020-24863**	GHTBSD-SA-20:01.txt, https://www.freebsd.org/security/advisories/FreeBSD-EN-20:18.getfsstat.asc	
HP					
hp-ux					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 184433. **CVE ID : CVE-2020-4578**	https://www.ibm.com/support/pages/node/6328895	O-HP-HP-U-180920/528
Huawei					
honor_view_20_firmware					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than	N/A	O-HUA-HONO-180920/529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
honor_20_pro_firmware					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than	N/A	O-HUA-HONO-180920/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can lead to information leak. **CVE ID : CVE-2020-9235**		
oxfords-an00a_firmware					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Vers	N/A	O-HUA-OXFO-180920/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
b2368-22_firmware					
Improper Control of Generation of Code ('Code Injection')	03-Sep-20	7.7	B2368-22 V100R001C00;B2368-57 V100R001C00;B2368-66 V100R001C00 have a command injection vulnerability. An attacker with high privileges may exploit this vulnerability through some operations on the LAN. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject commands to the target device. **CVE ID : CVE-2020-9199**	N/A	O-HUA-B236-180920/532
b2368-57_firmware					
Improper Control of Generation of Code ('Code Injection')	03-Sep-20	7.7	B2368-22 V100R001C00;B2368-57 V100R001C00;B2368-66 V100R001C00 have a command injection vulnerability. An attacker with high privileges may exploit this vulnerability through some operations on the LAN. Due to insufficient input validation of some	N/A	O-HUA-B236-180920/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameters, the attacker can exploit this vulnerability to inject commands to the target device. **CVE ID : CVE-2020-9199**		
b2368-66_firmware					
Improper Control of Generation of Code ('Code Injection')	03-Sep-20	7.7	B2368-22 V100R001C00;B2368-57 V100R001C00;B2368-66 V100R001C00 have a command injection vulnerability. An attacker with high privileges may exploit this vulnerability through some operations on the LAN. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject commands to the target device. **CVE ID : CVE-2020-9199**	N/A	O-HUA-B236-180920/534
yale-al00a_firmware					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than	N/A	O-HUA-YALE-180920/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
yale-l21a_firmware					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than	N/A	O-HUA-YALE-180920/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
yale-l61a_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a	N/A	O-HUA-YALE-180920/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
princeton-al10b_firmware					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versi	N/A	O-HUA-PRIN-180920/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ons earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
princeton-al10d_firmware					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);V	N/A	O-HUA-PRIN-180920/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ersions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
princeton-tl10c_firmware					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Vers	N/A	O-HUA-PRIN-180920/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
tony-al00b_firmware					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Vers	N/A	O-HUA-TONY-180920/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
mate_20_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	03-Sep-20	2.1	HUAWEI Mate 20 smart phones with Versions earlier than 10.1.0.163(C00E160R3P8) have a denial of service (DoS) vulnerability. The attacker can enter a large amount of text on the phone. Due to insufficient verification of the parameter, successful exploitation can impact the service. **CVE ID : CVE-2020-9083**	N/A	O-HUA-MATE-180920/542
IBM					
AIX					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 184433. **CVE ID : CVE-2020-4578**	https://www.ibm.com/support/pages/node/6328895	O-IBM-AIX-180920/543
Improper Input Validation	02-Sep-20	7.5	IBM Spectrum Protect Operations Center 7.1.0.000 through 7.1.10 and 8.1.0.000 through 8.1.9 may allow an attacker to execute arbitrary code on the system, caused by improper validation of data prior to export. IBM X-Force ID: 186782. **CVE ID : CVE-2020-4693**	https://www.ibm.com/support/pages/node/6325341	O-IBM-AIX-180920/544
i					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 184433. **CVE ID : CVE-2020-4578**	https://www.ibm.com/support/pages/node/6328895	O-IBM-I-180920/545
z\/os					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 184433. **CVE ID : CVE-2020-4578**	https://www.ibm.com/support/pages/node/6328895	O-IBM-Z\/O-180920/546
Lenovo					
thinkpad_a285_firmware					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the	N/A	O-LEN-THIN-180920/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**		
thinkpad_a485_firmware					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	O-LEN-THIN-180920/548
thinkpad_x1_carbon_\(20bx\)_firmware					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	O-LEN-THIN-180920/549
thinkpad_x395_firmware					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to	N/A	O-LEN-THIN-180920/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**		
thinkpad_t495_drift_firmware					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	O-LEN-THIN-180920/551
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	O-LEN-THIN-180920/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_t495s_jazz_firmware					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	O-LEN-THIN-180920/553
thinkpad_a275_firmware					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	O-LEN-THIN-180920/554
thinkpad_a475_firmware					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the	N/A	O-LEN-THIN-180920/555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**		
thinkpad_t490_\(20nx\)_firmware					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	O-LEN-THIN-180920/556
thinkpad_t490_\(20qx\)_firmware					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	O-LEN-THIN-180920/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_t490_\(20rx\)_firmware					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	O-LEN-THIN-180920/558
thinkpad_t490s_\(20nx\)_firmware					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	O-LEN-THIN-180920/559
thinkpad_t590_\(20nx\)_firmware					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash.	N/A	O-LEN-THIN-180920/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**		
thinkpad_x1_carbon_\(20qx\)_firmware					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	O-LEN-THIN-180920/561
thinkpad_x1_yoga_\(20qx\)_firmware					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3	N/A	O-LEN-THIN-180920/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**		
thinkpad_x390_\(20qx\)_firmware					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	O-LEN-THIN-180920/563
thinkpad_x390_\(20sx\)_firmware					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write	N/A	O-LEN-THIN-180920/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**		
Linux					
linux_kernel					
Use After Free	03-Sep-20	4.9	A flaw was found in the Linux kernel's implementation of GRO in versions before 5.2. This flaw allows an attacker with local access to crash the system. **CVE ID : CVE-2020-10720**	N/A	O-LIN-LINU-180920/565
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	3.6	In the Linux kernel through 5.8.7, local attackers able to inject conntrack netlink configuration could overflow a local buffer, causing crashes or triggering use of incorrect protocol numbers in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c, aka CID-1cc5ef91d2ff. **CVE ID : CVE-2020-25211**	N/A	O-LIN-LINU-180920/566
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Sep-20	4.4	A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt memory or possibly have unspecified other impact because a size check is in fs/nfs/nfs4proc.c instead of fs/nfs/nfs4xdr.c, aka CID-b4487b935452. **CVE ID : CVE-2020-25212**	N/A	O-LIN-LINU-180920/567
Use After Free	10-Sep-20	7.2	The Linux kernel 4.9.x before 4.9.233, 4.14.x before 4.14.194, and 4.19.x before	N/A	O-LIN-LINU-180920/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.19.140 has a use-after-free because skcd->no_refcnt was not considered during a backport of a CVE-2020-14356 patch. This is related to the cgroups feature. **CVE ID : CVE-2020-25220**		
Operation on a Resource after Expiration or Release	10-Sep-20	7.2	get_gate_page in mm/gup.c in the Linux kernel 5.7.x and 5.8.x before 5.8.7 allows privilege escalation because of incorrect reference counting (caused by gate page mishandling) of the struct page that backs the vsyscall page. The result is a refcount underflow. This can be triggered by any 64-bit process that can use ptrace() or process_vm_readv(), aka CID-9fa2dd946743. **CVE ID : CVE-2020-25221**	N/A	O-LIN-LINU-180920/569
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 184433. **CVE ID : CVE-2020-4578**	https://www.ibm.com/support/pages/node/6328895	O-LIN-LINU-180920/570
Improper Input Validation	02-Sep-20	7.5	IBM Spectrum Protect Operations Center 7.1.0.000 through 7.1.10 and 8.1.0.000 through 8.1.9 may allow an	https://www.ibm.com/support/pages/node/6325	O-LIN-LINU-180920/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code on the system, caused by improper validation of data prior to export. IBM X-Force ID: 186782. **CVE ID : CVE-2020-4693**	341	
Microsoft					
windows					
Insufficient Verification of Data Authenticity	04-Sep-20	5.8	In Foxit Reader and PhantomPDF before 10.0.1, and PhantomPDF before 9.7.3, attackers can obtain sensitive information about an uninitialized object because of direct transformation from PDF Object to Stream without concern for a crafted XObject. **CVE ID : CVE-2020-11493**	N/A	O-MIC-WIND-180920/572
Out-of-bounds Write	04-Sep-20	6.8	In Foxit Reader and PhantomPDF before 10.0.1, and PhantomPDF before 9.7.3, attackers can execute arbitrary code via a heap-based buffer overflow because dirty image-resource data is mishandled. **CVE ID : CVE-2020-12248**	N/A	O-MIC-WIND-180920/573
Improper Privilege Management	01-Sep-20	7.2	A vulnerability in Trend Micro Apex One and OfficeScan XG SP1 on Microsoft Windows may allow an attacker to create a hard link to any file on the system, which then could be manipulated to gain a privilege escalation and code execution. An attacker must first obtain the ability to execute low-privileged code	N/A	O-MIC-WIND-180920/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected. **CVE ID : CVE-2020-24556**		
Improper Privilege Management	01-Sep-20	7.2	A vulnerability in Trend Micro Apex One on Microsoft Windows may allow an attacker to manipulate a particular product folder to disable the security temporarily, abuse a specific Windows function and attain privilege escalation. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected. **CVE ID : CVE-2020-24557**	N/A	O-MIC-WIND-180920/575
Out-of-bounds Read	01-Sep-20	3.6	A vulnerability in an Trend Micro Apex One dll may allow an attacker to manipulate it to cause an out-of-bounds read that crashes multiple processes in the product. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	N/A	O-MIC-WIND-180920/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-24558		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 184433. **CVE ID : CVE-2020-4578**	https://www.ibm.com/support/pages/node/6328895	O-MIC-WIND-180920/577
Improper Input Validation	02-Sep-20	7.5	IBM Spectrum Protect Operations Center 7.1.0.000 through 7.1.10 and 8.1.0.000 through 8.1.9 may allow an attacker to execute arbitrary code on the system, caused by improper validation of data prior to export. IBM X-Force ID: 186782. **CVE ID : CVE-2020-4693**	https://www.ibm.com/support/pages/node/6325341	O-MIC-WIND-180920/578
Out-of-bounds Write	10-Sep-20	6.8	Adobe FrameMaker version 2019.0.6 (and earlier versions) lacks proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. This could be exploited to execute arbitrary code with the privileges of the current user. User interaction is required to exploit this vulnerability in that the target must open a malicious FrameMaker file.	N/A	O-MIC-WIND-180920/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9725		
Out-of-bounds Read	10-Sep-20	5.8	Adobe FrameMaker version 2019.0.6 (and earlier versions) has an out-of-bounds read vulnerability that could be exploited to read past the end of an allocated buffer, possibly resulting in a crash or disclosure of sensitive information from other memory locations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious FrameMaker file. **CVE ID : CVE-2020-9726**	N/A	O-MIC-WIND-180920/580
windows_10					
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1097. **CVE ID : CVE-2020-1091**	N/A	O-MIC-WIND-180920/581
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1033, CVE-2020-	N/A	O-MIC-WIND-180920/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1589, CVE-2020-1592. **CVE ID : CVE-2020-16854**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	7.6	A remote code execution vulnerability exists when the Windows Text Service Module improperly handles memory, aka 'Windows Text Service Module Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0908**	N/A	O-MIC-WIND-180920/583
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0914**	N/A	O-MIC-WIND-180920/584
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1033, CVE-2020-1589, CVE-2020-1592, CVE-2020-16854. **CVE ID : CVE-2020-0928**	N/A	O-MIC-WIND-180920/585
Information Exposure	11-Sep-20	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-2020-1250.	N/A	O-MIC-WIND-180920/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0941		
Incorrect Permission Assignment for Critical Resource	11-Sep-20	7.2	A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement, aka 'Windows Defender Application Control Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0951**	N/A	O-MIC-WIND-180920/587
Missing Authorization	11-Sep-20	2.1	An information disclosure vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0989**	N/A	O-MIC-WIND-180920/588
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	9.3	A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory, aka 'Windows Camera Codec Pack Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0997**	N/A	O-MIC-WIND-180920/589
Improper Privilege Management	11-Sep-20	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'.	N/A	O-MIC-WIND-180920/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0998		
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1589, CVE-2020-1592, CVE-2020-16854. **CVE ID : CVE-2020-1033**	N/A	O-MIC-WIND-180920/591
Improper Privilege Management	11-Sep-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1034**	N/A	O-MIC-WIND-180920/592
N/A	11-Sep-20	4.9	A denial of service vulnerability exists when Windows Routing Utilities improperly handles objects in memory, aka 'Windows Routing Utilities Denial of Service'. **CVE ID : CVE-2020-1038**	N/A	O-MIC-WIND-180920/593
N/A	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1074. **CVE ID : CVE-2020-1039**	N/A	O-MIC-WIND-180920/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists in the way that the ssdpsrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1159, CVE-2020-1376. **CVE ID : CVE-2020-1052**	N/A	O-MIC-WIND-180920/595
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1308. **CVE ID : CVE-2020-1053**	N/A	O-MIC-WIND-180920/596
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	9.3	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1172, CVE-2020-1180. **CVE ID : CVE-2020-1057**	N/A	O-MIC-WIND-180920/597
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1039. **CVE ID : CVE-2020-1074**	N/A	O-MIC-WIND-180920/598
Improper	11-Sep-20	2.1	An information disclosure	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0921. **CVE ID : CVE-2020-1083**		180920/599
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1091. **CVE ID : CVE-2020-1097**	N/A	O-MIC-WIND-180920/600
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Shell infrastructure component improperly handles objects in memory, aka 'Windows Shell Infrastructure Component Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1098**	N/A	O-MIC-WIND-180920/601
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege	N/A	O-MIC-WIND-180920/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1115**		
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when StartTileData.dll improperly handles objects in memory, aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1119**	N/A	O-MIC-WIND-180920/603
Improper Check for Unusual or Exceptional Conditions	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Windows Language Pack Installer improperly handles file operations, aka 'Windows Language Pack Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1122**	N/A	O-MIC-WIND-180920/604
N/A	11-Sep-20	6.8	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1319. **CVE ID : CVE-2020-1129**	N/A	O-MIC-WIND-180920/605
windows_7					
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This	N/A	O-MIC-WIND-180920/606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2020-1097. **CVE ID : CVE-2020-1091**		
N/A	11-Sep-20	4.9	A denial of service vulnerability exists when Windows Routing Utilities improperly handles objects in memory, aka 'Windows Routing Utilities Denial of Service'. **CVE ID : CVE-2020-1038**	N/A	O-MIC-WIND-180920/607
N/A	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1074. **CVE ID : CVE-2020-1039**	N/A	O-MIC-WIND-180920/608
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists in the way that the ssdpsrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1159, CVE-2020-1376. **CVE ID : CVE-2020-1052**	N/A	O-MIC-WIND-180920/609
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	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'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-180920/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1039. **CVE ID : CVE-2020-1074**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0921. **CVE ID : CVE-2020-1083**	N/A	O-MIC-WIND-180920/611
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1091. **CVE ID : CVE-2020-1097**	N/A	O-MIC-WIND-180920/612
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1115**	N/A	O-MIC-WIND-180920/613
windows_8.1					
Improper Control of Dynamicall	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component	N/A	O-MIC-WIND-180920/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
y-Managed Code Resources			improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1097. **CVE ID : CVE-2020-1091**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1033, CVE-2020-1589, CVE-2020-1592. **CVE ID : CVE-2020-16854**	N/A	O-MIC-WIND-180920/615
Information Exposure	11-Sep-20	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-2020-1250. **CVE ID : CVE-2020-0941**	N/A	O-MIC-WIND-180920/616
Improper Privilege Management	11-Sep-20	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'. **CVE ID : CVE-2020-0998**	N/A	O-MIC-WIND-180920/617
N/A	11-Sep-20	2.1	An information disclosure	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1589, CVE-2020-1592, CVE-2020-16854. **CVE ID : CVE-2020-1033**		180920/618
Improper Privilege Management	11-Sep-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1034**	N/A	O-MIC-WIND-180920/619
N/A	11-Sep-20	4.9	A denial of service vulnerability exists when Windows Routing Utilities improperly handles objects in memory, aka 'Windows Routing Utilities Denial of Service'. **CVE ID : CVE-2020-1038**	N/A	O-MIC-WIND-180920/620
N/A	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1074. **CVE ID : CVE-2020-1039**	N/A	O-MIC-WIND-180920/621
Improper Privilege	11-Sep-20	4.6	An elevation of privilege vulnerability exists in the way	N/A	O-MIC-WIND-180920/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			that the ssdpsrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1159, CVE-2020-1376. **CVE ID : CVE-2020-1052**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1039. **CVE ID : CVE-2020-1074**	N/A	O-MIC-WIND-180920/623
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0921. **CVE ID : CVE-2020-1083**	N/A	O-MIC-WIND-180920/624
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1091.	N/A	O-MIC-WIND-180920/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1097		
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1115**	N/A	O-MIC-WIND-180920/626
windows_rt_8.1					
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1097. **CVE ID : CVE-2020-1091**	N/A	O-MIC-WIND-180920/627
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1033, CVE-2020-1589, CVE-2020-1592. **CVE ID : CVE-2020-16854**	N/A	O-MIC-WIND-180920/628
Information Exposure	11-Sep-20	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel	N/A	O-MIC-WIND-180920/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1250. **CVE ID : CVE-2020-0941**		
Improper Privilege Management	11-Sep-20	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'. **CVE ID : CVE-2020-0998**	N/A	O-MIC-WIND-180920/630
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1589, CVE-2020-1592, CVE-2020-16854. **CVE ID : CVE-2020-1033**	N/A	O-MIC-WIND-180920/631
Improper Privilege Management	11-Sep-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1034**	N/A	O-MIC-WIND-180920/632
N/A	11-Sep-20	4.9	A denial of service vulnerability exists when Windows Routing Utilities improperly handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-180920/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Routing Utilities Denial of Service'. **CVE ID : CVE-2020-1038**		
N/A	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1074. **CVE ID : CVE-2020-1039**	N/A	O-MIC-WIND-180920/634
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists in the way that the ssdpsrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1159, CVE-2020-1376. **CVE ID : CVE-2020-1052**	N/A	O-MIC-WIND-180920/635
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1039. **CVE ID : CVE-2020-1074**	N/A	O-MIC-WIND-180920/636
Improper Restriction of Operations within the Bounds of a	11-Sep-20	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics	N/A	O-MIC-WIND-180920/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0921. **CVE ID : CVE-2020-1083**		
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1091. **CVE ID : CVE-2020-1097**	N/A	O-MIC-WIND-180920/638
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1115**	N/A	O-MIC-WIND-180920/639
windows_server_2008					
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1097. **CVE ID : CVE-2020-1091**	N/A	O-MIC-WIND-180920/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Sep-20	4.9	A denial of service vulnerability exists when Windows Routing Utilities improperly handles objects in memory, aka 'Windows Routing Utilities Denial of Service'. **CVE ID : CVE-2020-1038**	N/A	O-MIC-WIND-180920/641
N/A	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1074. **CVE ID : CVE-2020-1039**	N/A	O-MIC-WIND-180920/642
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists in the way that the ssdpsrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1159, CVE-2020-1376. **CVE ID : CVE-2020-1052**	N/A	O-MIC-WIND-180920/643
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1039. **CVE ID : CVE-2020-1074**	N/A	O-MIC-WIND-180920/644
Improper	11-Sep-20	2.1	An information disclosure	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0921. **CVE ID : CVE-2020-1083**		180920/645
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1091. **CVE ID : CVE-2020-1097**	N/A	O-MIC-WIND-180920/646
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1115**	N/A	O-MIC-WIND-180920/647
windows_server_2012					
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics	N/A	O-MIC-WIND-180920/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1097. **CVE ID : CVE-2020-1091**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1033, CVE-2020-1589, CVE-2020-1592. **CVE ID : CVE-2020-16854**	N/A	O-MIC-WIND-180920/649
Information Exposure	11-Sep-20	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-2020-1250. **CVE ID : CVE-2020-0941**	N/A	O-MIC-WIND-180920/650
Improper Privilege Management	11-Sep-20	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'. **CVE ID : CVE-2020-0998**	N/A	O-MIC-WIND-180920/651
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory,	N/A	O-MIC-WIND-180920/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1589, CVE-2020-1592, CVE-2020-16854. **CVE ID : CVE-2020-1033**		
Improper Privilege Management	11-Sep-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1034**	N/A	O-MIC-WIND-180920/653
N/A	11-Sep-20	4.9	A denial of service vulnerability exists when Windows Routing Utilities improperly handles objects in memory, aka 'Windows Routing Utilities Denial of Service'. **CVE ID : CVE-2020-1038**	N/A	O-MIC-WIND-180920/654
N/A	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1074. **CVE ID : CVE-2020-1039**	N/A	O-MIC-WIND-180920/655
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists in the way that the ssdpsrv.dll handles objects in memory, aka 'Windows Elevation of	N/A	O-MIC-WIND-180920/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1159, CVE-2020-1376. **CVE ID : CVE-2020-1052**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1039. **CVE ID : CVE-2020-1074**	N/A	O-MIC-WIND-180920/657
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0921. **CVE ID : CVE-2020-1083**	N/A	O-MIC-WIND-180920/658
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1091. **CVE ID : CVE-2020-1097**	N/A	O-MIC-WIND-180920/659
Improper Privilege	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-180920/660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1115**		
windows_server_2016					
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1097. **CVE ID : CVE-2020-1091**	N/A	O-MIC-WIND-180920/661
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1033, CVE-2020-1589, CVE-2020-1592. **CVE ID : CVE-2020-16854**	N/A	O-MIC-WIND-180920/662
Improper Restriction of Operations within the Bounds of a Memory	11-Sep-20	7.6	A remote code execution vulnerability exists when the Windows Text Service Module improperly handles memory, aka 'Windows Text Service Module Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-180920/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			**CVE ID : CVE-2020-0908**		
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0914**	N/A	O-MIC-WIND-180920/664
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1033, CVE-2020-1589, CVE-2020-1592, CVE-2020-16854. **CVE ID : CVE-2020-0928**	N/A	O-MIC-WIND-180920/665
Information Exposure	11-Sep-20	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-2020-1250. **CVE ID : CVE-2020-0941**	N/A	O-MIC-WIND-180920/666
Incorrect Permission Assignment for Critical Resource	11-Sep-20	7.2	A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement, aka 'Windows Defender Application Control Security	N/A	O-MIC-WIND-180920/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0951**		
Missing Authorization	11-Sep-20	2.1	An information disclosure vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0989**	N/A	O-MIC-WIND-180920/668
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	9.3	A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory, aka 'Windows Camera Codec Pack Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0997**	N/A	O-MIC-WIND-180920/669
Improper Privilege Management	11-Sep-20	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'. **CVE ID : CVE-2020-0998**	N/A	O-MIC-WIND-180920/670
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928,	N/A	O-MIC-WIND-180920/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1589, CVE-2020-1592, CVE-2020-16854. **CVE ID : CVE-2020-1033**		
Improper Privilege Management	11-Sep-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1034**	N/A	O-MIC-WIND-180920/672
N/A	11-Sep-20	4.9	A denial of service vulnerability exists when Windows Routing Utilities improperly handles objects in memory, aka 'Windows Routing Utilities Denial of Service'. **CVE ID : CVE-2020-1038**	N/A	O-MIC-WIND-180920/673
N/A	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1074. **CVE ID : CVE-2020-1039**	N/A	O-MIC-WIND-180920/674
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists in the way that the ssdpsrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1159, CVE-2020-1376. **CVE ID : CVE-2020-1052**	N/A	O-MIC-WIND-180920/675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1308. **CVE ID : CVE-2020-1053**	N/A	O-MIC-WIND-180920/676
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	9.3	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1172, CVE-2020-1180. **CVE ID : CVE-2020-1057**	N/A	O-MIC-WIND-180920/677
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1039. **CVE ID : CVE-2020-1074**	N/A	O-MIC-WIND-180920/678
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0921.	N/A	O-MIC-WIND-180920/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1083		
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1091. **CVE ID : CVE-2020-1097**	N/A	O-MIC-WIND-180920/680
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1115**	N/A	O-MIC-WIND-180920/681
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when StartTileData.dll improperly handles objects in memory, aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1119**	N/A	O-MIC-WIND-180920/682
Improper Check for Unusual or Exceptional Conditions	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Windows Language Pack Installer improperly handles file operations, aka 'Windows Language Pack Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1122**	N/A	O-MIC-WIND-180920/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Sep-20	6.8	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1319. **CVE ID : CVE-2020-1129**	N/A	O-MIC-WIND-180920/684
windows_server_2019					
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1097. **CVE ID : CVE-2020-1091**	N/A	O-MIC-WIND-180920/685
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1033, CVE-2020-1589, CVE-2020-1592. **CVE ID : CVE-2020-16854**	N/A	O-MIC-WIND-180920/686
Improper Restriction of Operations	11-Sep-20	7.6	A remote code execution vulnerability exists when the Windows Text Service Module improperly handles memory,	N/A	O-MIC-WIND-180920/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			aka 'Windows Text Service Module Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0908**		
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0914**	N/A	O-MIC-WIND-180920/688
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1033, CVE-2020-1589, CVE-2020-1592, CVE-2020-16854. **CVE ID : CVE-2020-0928**	N/A	O-MIC-WIND-180920/689
Information Exposure	11-Sep-20	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-2020-1250. **CVE ID : CVE-2020-0941**	N/A	O-MIC-WIND-180920/690
Incorrect Permission Assignment for Critical Resource	11-Sep-20	7.2	A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker	N/A	O-MIC-WIND-180920/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to bypass WDAC enforcement, aka 'Windows Defender Application Control Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0951**		
Missing Authorization	11-Sep-20	2.1	An information disclosure vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0989**	N/A	O-MIC-WIND-180920/692
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	9.3	A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory, aka 'Windows Camera Codec Pack Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0997**	N/A	O-MIC-WIND-180920/693
Improper Privilege Management	11-Sep-20	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'. **CVE ID : CVE-2020-0998**	N/A	O-MIC-WIND-180920/694
N/A	11-Sep-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel	N/A	O-MIC-WIND-180920/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0928, CVE-2020-1589, CVE-2020-1592, CVE-2020-16854. **CVE ID : CVE-2020-1033**		
Improper Privilege Management	11-Sep-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1034**	N/A	O-MIC-WIND-180920/696
N/A	11-Sep-20	4.9	A denial of service vulnerability exists when Windows Routing Utilities improperly handles objects in memory, aka 'Windows Routing Utilities Denial of Service'. **CVE ID : CVE-2020-1038**	N/A	O-MIC-WIND-180920/697
N/A	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1074. **CVE ID : CVE-2020-1039**	N/A	O-MIC-WIND-180920/698
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists in the way that the ssdpsrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-180920/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2020-1159, CVE-2020-1376. **CVE ID : CVE-2020-1052**		
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1308. **CVE ID : CVE-2020-1053**	N/A	O-MIC-WIND-180920/700
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	9.3	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1172, CVE-2020-1180. **CVE ID : CVE-2020-1057**	N/A	O-MIC-WIND-180920/701
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Sep-20	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'. This CVE ID is unique from CVE-2020-1039. **CVE ID : CVE-2020-1074**	N/A	O-MIC-WIND-180920/702
Improper Restriction of Operations within the Bounds of a Memory	11-Sep-20	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information	N/A	O-MIC-WIND-180920/703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0921. **CVE ID : CVE-2020-1083**		
Improper Control of Dynamically-Managed Code Resources	11-Sep-20	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1091. **CVE ID : CVE-2020-1097**	N/A	O-MIC-WIND-180920/704
Improper Privilege Management	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1115**	N/A	O-MIC-WIND-180920/705
Improper Check for Unusual or Exceptional Conditions	11-Sep-20	4.6	An elevation of privilege vulnerability exists when the Windows Language Pack Installer improperly handles file operations, aka 'Windows Language Pack Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1122**	N/A	O-MIC-WIND-180920/706
N/A	11-Sep-20	6.8	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles	N/A	O-MIC-WIND-180920/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1319. **CVE ID : CVE-2020-1129**		
Netgear					
r8300_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Sep-20	5.8	NETGEAR R8300 devices before 1.0.2.134 are affected by command injection by an unauthenticated attacker. **CVE ID : CVE-2020-25067**	N/A	O-NET-R830-180920/708
Opensuse					
leap					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	02-Sep-20	4	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Splitting attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the browser cache and any downstream caches with content from an arbitrary source. Squid uses a string search instead of parsing the	N/A	O-OPE-LEAP-180920/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Transfer-Encoding header to find chunked encoding. This allows an attacker to hide a second request inside Transfer-Encoding: it is interpreted by Squid as chunked and split out into a second request delivered upstream. Squid will then deliver two distinct responses to the client, corrupting any downstream caches. **CVE ID : CVE-2020-15811**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Sep-20	4.3	In KDE Ark before 20.08.1, a crafted TAR archive with symlinks can install files outside the extraction directory, as demonstrated by a write operation to a user's home directory. **CVE ID : CVE-2020-24654**	https://bugzilla.suse.com/show_bug.cgi?id=1175857, https://github.com/KDE/ark/commit/8bf8c5ef07b0ac5e914d752681e470dea403a5bd, https://kde.org/info/security/advisory-20200827-1.txt	O-OPE-LEAP-180920/710
Acceptance of Extraneous Untrusted Data With Trusted Data	01-Sep-20	7.2	A acceptance of Extraneous Untrusted Data With Trusted Data vulnerability in the start script of openldap2 of SUSE Enterprise Storage 5, SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise	https://bugzilla.suse.com/show_bug.cgi?id=1172698	O-OPE-LEAP-180920/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server 11-SECURITY, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to escalate privileges from user ldap to root. This issue affects: SUSE Enterprise Storage 5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Debuginfo 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Debuginfo 11-SP4 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Point of Sale 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 11-SECURITY openldap2-client-openssl1 versions prior to 2.4.26-0.74.13.1. SUSE Linux		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Server 11-SP4-LTSS openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 12-SP2-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP2-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP4 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.31.1. SUSE Linux Enterprise Server for SAP 12-SP2 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 12-SP3 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.31.1. SUSE OpenStack Cloud 7 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud 8 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud Crowbar 8 openldap2 versions prior to 2.4.41-18.71.2. openSUSE Leap 15.1		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			openldap2 versions prior to 2.4.46-lp151.10.12.1. openSUSE Leap 15.2 openldap2 versions prior to 2.4.46-lp152.14.3.1. **CVE ID : CVE-2020-8023**		
Oracle					
solaris					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-20	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 184433. **CVE ID : CVE-2020-4578**	https://www.ibm.com/support/pages/node/6328895	O-ORA-SOLA-180920/712
Paloaltonetworks					
pan-os					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-20	6.8	A reflected cross-site scripting (XSS) vulnerability exists in the PAN-OS management web interface. A remote attacker able to convince an administrator with an active authenticated session on the firewall management interface to click on a crafted link to that management web interface could potentially execute arbitrary JavaScript code in the administrator's browser and perform administrative actions. This	N/A	O-PAL-PAN--180920/713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9. **CVE ID : CVE-2020-2036**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Sep-20	9	An OS Command Injection vulnerability in the PAN-OS management interface that allows authenticated administrators to execute arbitrary OS commands with root privileges. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.3. **CVE ID : CVE-2020-2037**	N/A	O-PAL-PAN--180920/714
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Sep-20	9	An OS Command Injection vulnerability in the PAN-OS management interface that allows authenticated administrators to execute arbitrary OS commands with root privileges. This issue impacts: PAN-OS 9.0 versions earlier than 9.0.10; PAN-OS 9.1 versions earlier than 9.1.4; PAN-OS 10.0 versions earlier than 10.0.1. **CVE ID : CVE-2020-2038**	N/A	O-PAL-PAN--180920/715
Uncontrolled Resource Consumption	09-Sep-20	5	An uncontrolled resource consumption vulnerability in Palo Alto Networks PAN-OS allows for a remote unauthenticated user to upload temporary files through the management web	N/A	O-PAL-PAN--180920/716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface that are not properly deleted after the request is finished. It is possible for an attacker to disrupt the availability of the management web interface by repeatedly uploading files until available disk space is exhausted. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.4; PAN-OS 10.0 versions earlier than PAN-OS 10.0.1. **CVE ID : CVE-2020-2039**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	10	A buffer overflow vulnerability in PAN-OS allows an unauthenticated attacker to disrupt system processes and potentially execute arbitrary code with root privileges by sending a malicious request to the Captive Portal or Multi-Factor Authentication interface. This issue impacts: All versions of PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 9.1 versions earlier than PAN-OS 9.1.3. **CVE ID : CVE-2020-2040**	N/A	O-PAL-PAN--180920/717
N/A	09-Sep-20	7.8	An insecure configuration of the appweb daemon of Palo Alto Networks PAN-OS 8.1 allows a remote unauthenticated user to send a	N/A	O-PAL-PAN--180920/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted request to the device that causes the appweb service to crash. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode. This issue impacts all versions of PAN-OS 8.0, and PAN-OS 8.1 versions earlier than 8.1.16. **CVE ID : CVE-2020-2041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	9	A buffer overflow vulnerability in the PAN-OS management web interface allows authenticated administrators to disrupt system processes and potentially execute arbitrary code with root privileges. This issue impacts only PAN-OS 10.0 versions earlier than PAN-OS 10.0.1. **CVE ID : CVE-2020-2042**	N/A	O-PAL-PAN--180920/719
Information Exposure Through Log Files	09-Sep-20	4	An information exposure through log file vulnerability where sensitive fields are recorded in the configuration log without masking on Palo Alto Networks PAN-OS software when the after-change-detail custom syslog field is enabled for configuration logs and the sensitive field appears multiple times in one log entry. The first instance of the sensitive field is masked but	N/A	O-PAL-PAN--180920/720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subsequent instances are left in clear text. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.4. **CVE ID : CVE-2020-2043**		
Information Exposure Through Log Files	09-Sep-20	4	An information exposure through log file vulnerability where an administrator's password or other sensitive information may be logged in cleartext while using the CLI in Palo Alto Networks PAN-OS software. The opcmdhistory.log file was introduced to track operational command (op-command) usage but did not mask all sensitive information. The opcmdhistory.log file is removed in PAN-OS 9.1 and later PAN-OS versions. Command usage is recorded, instead, in the req_stats.log file in PAN-OS 9.1 and later PAN-OS versions. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.3. **CVE ID : CVE-2020-2044**	N/A	O-PAL-PAN--180920/721
Philips					
intellivue_mp2-mp90_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	O-PHI-INTE-180920/722
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	O-PHI-INTE-180920/723
intellivue_mx100_firmware					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100,	N/A	O-PHI-INTE-180920/724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	O-PHI-INTE-180920/725
intellivue_mx400_firmware					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does	N/A	O-PHI-INTE-180920/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	O-PHI-INTE-180920/727
intellivue_mx850_firmware					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-	N/A	O-PHI-INTE-180920/728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service condition through a system restart. **CVE ID : CVE-2020-16216**		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	O-PHI-INTE-180920/729
intellivue_x2_firmware					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	O-PHI-INTE-180920/730
Improper	11-Sep-20	5.2	Patient Information Center iX	N/A	O-PHI-INTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Check for Certificate Revocation			(PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**		180920/731
intellivue_x3_firmware					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	O-PHI-INTE-180920/732
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-	N/A	O-PHI-INTE-180920/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**		
intellivue_mx800_firmware					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	O-PHI-INTE-180920/734
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of	N/A	O-PHI-INTE-180920/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**		
intellivue_mx750_firmware					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	O-PHI-INTE-180920/736
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	O-PHI-INTE-180920/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
intellivue_mx700_firmware					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	O-PHI-INTE-180920/738
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	O-PHI-INTE-180920/739
intellivue_mx600_firmware					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue	N/A	O-PHI-INTE-180920/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	O-PHI-INTE-180920/741
intellivue_mx550_firmware					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product	N/A	O-PHI-INTE-180920/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	O-PHI-INTE-180920/743
Qualcomm					
qca6574au_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qcs405_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/749
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of	https://www.qualcomm.com/compan	O-QUA-QCS4-180920/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	y/product-security/bulletins/august-2020-bulletin	
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/751

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 APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS4-180920/752
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-QCS4-180920/753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' 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/august-2020-bulletin	O-QUA-QCS4-180920/755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure	https://www.qualcomm.	O-QUA-QCS4-180920/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	com/company/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS4-180920/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	etins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**		
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/760
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS4-180920/761
Out-of-bounds	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host	https://www.qualcomm.com/compan	O-QUA-QCS4-180920/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	y/product-security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-QCS4-180920/763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/765
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS4-180920/766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/767
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**		
ipq4019_firmware					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ4-180920/769
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ4-180920/770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ4-180920/771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**		
ipq8064_firmware					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/772
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**		
ipq8074_firmware					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/775
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/782
Improper	08-Sep-20	10	u'Buffer Overflow issue in	https://ww	O-QUA-IPQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/783
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ8-180920/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
qca6174a_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/786
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of	https://www.qualcomm.com/compan	O-QUA-QCA6-180920/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	y/product-security/bulletins/august-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca9377_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca9379_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/794
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header	https://www.qualcomm.	O-QUA-QCA9-180920/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	com/company/product-security/bulletins/august-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-QCA9-180920/796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	bulletin	
sdm429w_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11128		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM4-180920/805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/807
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM4-180920/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
sc7180_firmware					
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SC71-180920/809
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' 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/august-2020-bulletin	O-QUA-SC71-180920/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow	https://www.qualcomm.	O-QUA-SC71-180920/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3624		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/815
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SC71-180920/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/817
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3643		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/820
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SC71-180920/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/823
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC71-180920/824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SC71-180920/825
apq8009_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-APQ8-180920/826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/830
Integer Overflow or	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round	https://www.qualcomm.	O-QUA-APQ8-180920/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-APQ8-180920/837
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
apq8098_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/842
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/844
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-	O-QUA-APQ8-180920/845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	bulletin	
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/846
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' 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/august-2020-bulletin	O-QUA-APQ8-180920/849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow	https://www.qualcomm.	O-QUA-APQ8-180920/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3624		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-APQ8-180920/852
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-APQ8-180920/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3667		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/857
msm8953_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/861
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer	https://www.qualcomm.com/company/product-	O-QUA-MSM8-180920/862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	security/bulletins/august-2020-bulletin	
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MSM8-180920/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11135		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/864
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-MSM8-180920/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**	-2020-bulletin	
Improper	08-Sep-20	4.9	u'Lack of check to ensure that	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	MSM8-180920/866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MSM8-180920/869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3643		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MSM8-180920/871
msm8998_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/874
Improper Validation	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file	https://www.qualcomm.	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Array Index			content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	com/company/product-security/bulletins/august-2020-bulletin	180920/875
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/876
Improper	08-Sep-20	4.6	u'XBL SEC clears only ZI	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	MSM8-180920/877
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MSM8-180920/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/887
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' 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/august-2020-bulletin	O-QUA-MSM8-180920/888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
nicobar_firmware					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-NICO-180920/889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-NICO-180920/890
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-NICO-180920/891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-NICO-180920/892
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-NICO-180920/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-NICO-180920/894

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string	https://www.qualcomm.com/company/product-	O-QUA-NICO-180920/895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-NICO-180920/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-NICO-180920/897
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-	https://www.qualcomm.com/compan	O-QUA-NICO-180920/898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	y/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-NICO-180920/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-NICO-180920/900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-NICO-180920/901
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-NICO-180920/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-NICO-180920/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-NICO-180920/904
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-NICO-180920/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3675		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-NICO-180920/906
apq8053_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-APQ8-180920/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/918
mdm9207c_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
msm8905_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11116		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/926
Time-of-check Time-of-use (TOCTOU)	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege	https://www.qualcomm.com/company/product-	O-QUA-MSM8-180920/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Race Condition			escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	security/bulletins/august-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-MSM8-180920/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**	-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MSM8-180920/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/933
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is	https://www.qualcomm.com/compan	O-QUA-MSM8-180920/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	y/product-security/bulletins/august-2020-bulletin	
qcn7605_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCN7-180920/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCN7-180920/936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCN7-180920/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCN7-180920/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCN7-180920/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCN7-180920/940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' 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/august-2020-bulletin	O-QUA-QCN7-180920/941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCN7-180920/942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCN7-180920/943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCN7-180920/944
sdm845_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/948
Buffer Copy	08-Sep-20	4.6	u'Possible out of bound array	https://ww	O-QUA-SDM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/949
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/950
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SDM8-180920/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**	bulletin	
Integer	08-Sep-20	4.6	u'A potential buffer overflow	https://ww	O-QUA-SDM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/956
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM8-180920/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM8-180920/960
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/963
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
apq8076_firmware					
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
ipq5018_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ5-180920/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ5-180920/967
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ5-180920/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
apq8017_firmware					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/970
Improper Input	08-Sep-20	4.6	u'Channel name string which has been read from shared	https://www.qualcomm.	O-QUA-APQ8-180920/971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
apq8096au_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/975
Buffer Copy without Checking Size of Input	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-APQ8-180920/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	etins/august-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/979
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-	https://www.qualcomm.com/company/product-	O-QUA-APQ8-180920/980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3620		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-APQ8-180920/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-APQ8-180920/986
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-APQ8-180920/987

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 Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	security/bulletins/august-2020-bulletin	
sda845_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SDA8-180920/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/990
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SDA8-180920/991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDA8-180920/997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/1000
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/1001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/1002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/1003
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA8-180920/1004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
sdm636_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1007
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1008
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SDM6-180920/1009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	-2020-bulletin	
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1010
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SDM6-180920/1014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**	bulletin	
Integer	08-Sep-20	4.6	u'A potential buffer overflow	https://ww	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1016
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SDM6-180920/1017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1021
sdm670_firmware					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1024
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**		
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1026
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1028
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SDM6-180920/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**	bulletin	
Improper Restriction	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write	https://www.qualcomm.	O-QUA-SDM6-180920/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3643		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1035
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SDM6-180920/1036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1038
Improper	08-Sep-20	10	u'Buffer Overflow issue in	https://ww	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/1039
sdm710_firmware					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM7-180920/1042
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1043
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-	O-QUA-SDM7-180920/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	bulletin	
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1045
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM7-180920/1046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1047
Integer Overflow or	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round	https://www.qualcomm.	O-QUA-SDM7-180920/1048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM7-180920/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1054
Buffer Copy without Checking	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of	https://www.qualcomm.com/compan	O-QUA-SDM7-180920/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	y/product-security/bulletins/september-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3667		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1058
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM7-180920/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
sm6150_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11116		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1062
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop	https://www.qualcomm.com/company/product-	O-QUA-SM61-180920/1063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	security/bulletins/august-2020-bulletin	
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1064
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM61-180920/1065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1066
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by	https://www.qualcomm.	O-QUA-SM61-180920/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	com/company/product-security/bulletins/september-2020-bulletin	
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM61-180920/1068
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SM61-180920/1069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially	https://www.qualcomm.com/compan	O-QUA-SM61-180920/1072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	y/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1074
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM61-180920/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1076
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1079
Buffer Copy without Checking	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer	https://www.qualcomm.com/compan	O-QUA-SM61-180920/1080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	y/product-security/bulletins/august-2020-bulletin	
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1081
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM61-180920/1082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1083
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SM61-180920/1084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1086
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM61-180920/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM61-180920/1088
qm215_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-QM21-180920/1089

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 APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QM21-180920/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QM21-180920/1091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QM21-180920/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11120		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QM21-180920/1093
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QM21-180920/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QM21-180920/1095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QM21-180920/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QM21-180920/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QM21-180920/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QM21-180920/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QM21-180920/1100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QM21-180920/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QM21-180920/1102
qca6574_firmware					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/1103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca8081_firmware					
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA8-180920/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA8-180920/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' 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/august-2020-bulletin	O-QUA-QCA8-180920/1106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA8-180920/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Out-of-bounds	08-Sep-20	7.2	u'Out of bounds memory access during memory copy	https://www.qualcomm.	O-QUA-QCA8-180920/1108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	com/company/product-security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-QCA8-180920/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA8-180920/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA8-180920/1111
qcs404_firmware					
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS4-180920/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**		
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1113
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the	https://www.qualcomm.com/compan	O-QUA-QCS4-180920/1118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	y/product-security/bulletins/august-2020-bulletin	
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1119
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3667		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1124
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS4-180920/1126
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS4-180920/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	etins/september-2020-bulletin	
sm8150_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1131
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1132
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client	https://www.qualcomm.com/company/product-	O-QUA-SM81-180920/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	security/bulletins/september-2020-bulletin	
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11128		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM81-180920/1135
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM81-180920/1136
Time-of-check Time-of-use (TOCTOU)	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege	https://www.qualcomm.com/company/product-	O-QUA-SM81-180920/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Race Condition			escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	security/bulletins/august-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SM81-180920/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**	-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1142
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM81-180920/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1146
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1147
Buffer Copy without Checking Size of Input ('Classic	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/septem	O-QUA-SM81-180920/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	ber-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3667		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1150
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM81-180920/1152
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM81-180920/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM81-180920/1154
mdm9206_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MDM9-180920/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3666**		
mdm9607_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1167
Buffer Copy without	08-Sep-20	10	u'Possible out of bound write while processing association	https://www.qualcomm.	O-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	com/company/product-security/bulletins/august-2020-bulletin	180920/1168
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MDM9-180920/1170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1171
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-MDM9-180920/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially	https://www.qualcomm.com/compan	O-QUA-MDM9-180920/1175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	y/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MDM9-180920/1177
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-	https://www.qualcomm.com/compan	O-QUA-MDM9-180920/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	y/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-MDM9-180920/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	-2020-bulletin	
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1180
Buffer Copy without Checking	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of	https://www.qualcomm.com/compan	O-QUA-MDM9-180920/1181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	y/product-security/bulletins/september-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
mdm9650_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1186
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' 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/august-2020-bulletin	O-QUA-MDM9-180920/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow	https://www.qualcomm.	O-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	com/company/product-security/bulletins/august-2020-bulletin	180920/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3624		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MDM9-180920/1192
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-MDM9-180920/1193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
mdm9655_firmware					
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-MDM9-180920/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	-2020-bulletin	
Integer Underflow (Wrap or	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic	https://www.qualcomm.com/compan	O-QUA-MDM9-180920/1200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	y/product-security/bulletins/september-2020-bulletin	
msm8996au_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-MSM8-180920/1206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	-2020-bulletin	
Integer Underflow (Wrap or	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic	https://www.qualcomm.com/compan	O-QUA-MSM8-180920/1207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	y/product-security/bulletins/september-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1211
mdm9615_firmware					
Integer Overflow or	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow	https://www.qualcomm.	O-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	com/company/product-security/bulletins/august-2020-bulletin	180920/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3624		
mdm9625_firmware					
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MDM9-180920/1214
mdm9205_firmware					
Integer Overflow or	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round	https://www.qualcomm.	O-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	com/company/product-security/bulletins/august-2020-bulletin	180920/1215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MDM9-180920/1219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1221
msm8909_firmware					
Time-of-check	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during	https://www.qualcomm.	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	com/company/product-security/bulletins/august-2020-bulletin	180920/1222
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than	https://www.qualcomm.com/company/product-	O-QUA-MSM8-180920/1224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm9635m_firmware					
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MDM9-180920/1230
qca6584au_firmware					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host	https://www.qualcomm.com/compan	O-QUA-QCA6-180920/1231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	y/product-security/bulletins/august-2020-bulletin	
qca9531_firmware					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-QCA9-180920/1232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/1233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/1234
qca9880_firmware					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/1235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca9886_firmware					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/1236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca9980_firmware					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/1237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11117		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/1238
qcn5502_firmware					
Out-of-	08-Sep-20	7.2	u'Out of bounds memory	https://ww	O-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/1239
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-180920/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	etins/august-2020-bulletin	
sdm429_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1244
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM4-180920/1246
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SDM4-180920/1247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially	https://www.qualcomm.com/compan	O-QUA-SDM4-180920/1250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	y/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM4-180920/1252
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-	https://www.qualcomm.com/compan	O-QUA-SDM4-180920/1253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	y/product-security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/septem	O-QUA-SDM4-180920/1254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	ber-2020-bulletin	
sdm632_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11118		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1258
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1260
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SDM6-180920/1264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**	-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1266
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SDM6-180920/1267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
msm8917_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1271
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was	https://www.qualcomm.	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	com/company/product-security/bulletins/august-2020-bulletin	180920/1272
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MSM8-180920/1274
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparoun	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options	https://www.qualcomm.com/compan	O-QUA-MSM8-180920/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d			due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	y/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MSM8-180920/1280
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MSM8-180920/1282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
msm8920_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1285
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-MSM8-180920/1286

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 APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	etins/august-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-MSM8-180920/1291

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-MSM8-180920/1292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	security/bulletins/august-2020-bulletin	
msm8937_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-MSM8-180920/1293

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 APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1297
Integer	08-Sep-20	2.1	u'Lack of check of integer	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	MSM8-180920/1298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
msm8940_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1306
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' 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/august-2020-bulletin	O-QUA-MSM8-180920/1309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow	https://www.qualcomm.	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	com/company/product-security/bulletins/august-2020-bulletin	180920/1311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3624		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1312
msm8996_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
sdm450_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1319
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SDM4-180920/1320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	-2020-bulletin	
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11128		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM4-180920/1323
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM4-180920/1329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM4-180920/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3656		
sm8250_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1332
Buffer Copy without Checking	08-Sep-20	10	u'Possible out of bound write while processing association response received from host	https://www.qualcomm.com/compan	O-QUA-SM82-180920/1333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	y/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1336
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM82-180920/1337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1338
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM82-180920/1339
Reachable	09-Sep-20	7.8	u'Reachable assertion when	https://ww	O-QUA-SM82-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	w.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	180920/1340
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SM82-180920/1344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	bulletin	
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1345
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3643		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1348
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SM82-180920/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM82-180920/1350
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM82-180920/1353
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM82-180920/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM82-180920/1355
sxr2130_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1359
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SXR2-180920/1361
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SXR2-180920/1363
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SXR2-180920/1364
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SXR2-180920/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**	bulletin	
Improper Restriction	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write	https://www.qualcomm.	O-QUA-SXR2-180920/1366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1368
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**		
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1370
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR2-180920/1373
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SXR2-180920/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SXR2-180920/1375
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SXR2-180920/1376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**		
qca9563_firmware					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/1377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3666**		
qcn5500_firmware					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCN5-180920/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sa6155p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA61-180920/1379
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA61-180920/1380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	etins/august-2020-bulletin	
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SA61-180920/1381
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA61-180920/1382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SA61-180920/1383
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA61-180920/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than	https://www.qualcomm.com/company/product-	O-QUA-SA61-180920/1385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA61-180920/1386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA61-180920/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA61-180920/1388
Buffer Copy without Checking	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of	https://www.qualcomm.com/compan	O-QUA-SA61-180920/1389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	y/product-security/bulletins/september-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA61-180920/1390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SA61-180920/1391
sc8180x_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to	https://www.qualcomm.com/compan	O-QUA-SC81-180920/1392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	y/product-security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SC81-180920/1395
Improper Validation	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file	https://www.qualcomm.	O-QUA-SC81-180920/1396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Array Index			content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	com/company/product-security/bulletins/august-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially	https://www.qualcomm.com/compan	O-QUA-SC81-180920/1399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	y/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1402
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SC81-180920/1403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	-2020-bulletin	
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1404
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SC81-180920/1405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1406
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SC81-180920/1409
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SC81-180920/1410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SC81-180920/1411
sdm850_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1412
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SDM8-180920/1413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM8-180920/1419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1423
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM8-180920/1425
qcm2150_firmware					
Out-of-bounds	08-Sep-20	5	u'Buffer over read occurs while processing information	https://www.qualcomm.	O-QUA-QCM2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	com/company/product-security/bulletins/august-2020-bulletin	180920/1426
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCM2-180920/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCM2-180920/1428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCM2-180920/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCM2-180920/1430
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-	O-QUA-QCM2-180920/1431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCM2-180920/1432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCM2-180920/1433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCM2-180920/1434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCM2-180920/1435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCM2-180920/1436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCM2-180920/1437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCM2-180920/1438
Buffer Copy without Checking Size of	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value	https://www.qualcomm.com/company/product-	O-QUA-QCM2-180920/1439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	security/bulletins/september-2020-bulletin	
sdx55_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDX5-180920/1443
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDX5-180920/1449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1450
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDX5-180920/1451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	etins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3644		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1454
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1455
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDX5-180920/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDX5-180920/1457
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX5-180920/1458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDX5-180920/1459
sda660_firmware					
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA6-180920/1460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDA6-180920/1461
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA6-180920/1462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA6-180920/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA6-180920/1464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA6-180920/1465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage	https://www.qualcomm.com/company/product-	O-QUA-SDA6-180920/1466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	security/bulletins/august-2020-bulletin	
Integer	09-Sep-20	9.4	u'Multiple Read overflows	https://ww	O-QUA-SDA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	w.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	180920/1467
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA6-180920/1468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDA6-180920/1469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
sdm439_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1473
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM4-180920/1475
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1478

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string	https://www.qualcomm.com/company/product-	O-QUA-SDM4-180920/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM4-180920/1480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM4-180920/1481
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-	https://www.qualcomm.com/compan	O-QUA-SDM4-180920/1482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	y/product-security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/septem	O-QUA-SDM4-180920/1483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	ber-2020-bulletin	
sdm630_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1486
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1487
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access	https://www.qualcomm.com/company/product-	O-QUA-SDM6-180920/1488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	security/bulletins/august-2020-bulletin	
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1489
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1492

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDM6-180920/1493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	etins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3622		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1495
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SDM6-180920/1496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SDM6-180920/1497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1500
sdm660_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SDM6-180920/1501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1504
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SDM6-180920/1505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1506
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDM6-180920/1507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	etins/september-2020-bulletin	
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1508
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3619		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDM6-180920/1515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3644		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1518
Buffer Copy without Checking	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer	https://www.qualcomm.com/compan	O-QUA-SDM6-180920/1519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	y/product-security/bulletins/august-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDM6-180920/1520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
mdm9150_firmware					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1522
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-MDM9-180920/1523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially	https://www.qualcomm.com/compan	O-QUA-MDM9-180920/1526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	y/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MDM9-180920/1528
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-	https://www.qualcomm.com/compan	O-QUA-MDM9-180920/1529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	y/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-MDM9-180920/1530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	-2020-bulletin	
mdm9640_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MDM9-180920/1538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
msm8909w_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11118		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MSM8-180920/1544
Buffer Copy without Checking Size of	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in	https://www.qualcomm.com/company/product-	O-QUA-MSM8-180920/1545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	security/bulletins/august-2020-bulletin	
Improper Input Validation	08-Sep-20	4.6	u'Possible out of bound write in DSP driver code due to lack of check of data received from user' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W **CVE ID : CVE-2020-3648**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1546
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MSM8-180920/1547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**		
qcs605_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1550
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS6-180920/1551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	etins/august-2020-bulletin	
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS6-180920/1553
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1554
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS6-180920/1555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**		
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1556
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS6-180920/1557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3617		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1558
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-QCS6-180920/1559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**	-2020-bulletin	
Improper	08-Sep-20	4.9	u'Lack of check to ensure that	https://ww	O-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/1560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS6-180920/1563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3643		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1565
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-QCS6-180920/1566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS6-180920/1567
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1570
Improper	08-Sep-20	10	u'Buffer Overflow issue in	https://ww	O-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/1571
sdx20_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDX2-180920/1579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3702		
sm7150_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1582
Buffer Copy without Checking	08-Sep-20	10	u'Possible out of bound write while processing association response received from host	https://www.qualcomm.com/compan	O-QUA-SM71-180920/1583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	y/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1586
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM71-180920/1587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1588
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM71-180920/1589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM71-180920/1590
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-SM71-180920/1595

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	bulletin	
Buffer Copy without Checking Size of	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on	https://www.qualcomm.com/company/product-	O-QUA-SM71-180920/1596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	security/bulletins/august-2020-bulletin	
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM71-180920/1597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1598
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1599
Information	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure	https://www.qualcomm.	O-QUA-SM71-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	com/company/product-security/bulletins/august-2020-bulletin	180920/1600
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM71-180920/1601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	etins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**		
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1603
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM71-180920/1604
Buffer Copy without Checking	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer	https://www.qualcomm.com/compan	O-QUA-SM71-180920/1605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	y/product-security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SM71-180920/1607
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SM71-180920/1608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	-2020-bulletin	
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SM71-180920/1609
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN	https://www.qualcomm.com/compan	O-QUA-SM71-180920/1610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	y/product-security/bulletins/august-2020-bulletin	
sxr1130_firmware					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1613
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SXR1-180920/1614
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SXR1-180920/1615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	etins/august-2020-bulletin	
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SXR1-180920/1616
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SXR1-180920/1620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**	-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SXR1-180920/1622
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SXR1-180920/1623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1627
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SXR1-180920/1628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
sdx24_firmware					
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1630
Integer Overflow or	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round	https://www.qualcomm.	O-QUA-SDX2-180920/1631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SDX2-180920/1635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1637
Buffer Copy without Checking	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer	https://www.qualcomm.com/compan	O-QUA-SDX2-180920/1638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	y/product-security/bulletins/august-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SDX2-180920/1639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
rennell_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11118		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1642
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-RENN-180920/1643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11124**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1644
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-RENN-180920/1645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-RENN-180920/1646
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage	https://www.qualcomm.com/company/product-	O-QUA-RENN-180920/1651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	security/bulletins/august-2020-bulletin	
Buffer Copy	08-Sep-20	4.6	u'Stack out of bound issue	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	RENN-180920/1652
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-RENN-180920/1653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1654
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3640		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1656
Information	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic	https://www.qualcomm.	O-QUA-RENN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	com/company/product-security/bulletins/august-2020-bulletin	180920/1657
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-RENN-180920/1658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1659
Buffer Copy without Checking	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length	https://www.qualcomm.com/compan	O-QUA-RENN-180920/1660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	y/product-security/bulletins/august-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-RENN-180920/1662
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-RENN-180920/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**		
sa415m_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA41-180920/1664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA41-180920/1665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA41-180920/1666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA41-180920/1667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA41-180920/1668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA41-180920/1669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SA41-180920/1670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA41-180920/1671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA41-180920/1672
Buffer Copy	08-Sep-20	10	u'Buffer Overflow in mic	https://ww	O-QUA-SA41-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/1673
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA41-180920/1674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA41-180920/1675
Integer Underflow (Wrap or Wraparoun	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE	https://www.qualcomm.com/company/product-	O-QUA-SA41-180920/1676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	security/bulletins/august-2020-bulletin	
saipan_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1680
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1681
Use After	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table	https://www.qualcomm.	O-QUA-SAIP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	com/company/product-security/bulletins/september-2020-bulletin	180920/1682
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SAIP-180920/1684
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SAIP-180920/1685
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than	https://www.qualcomm.com/company/product-	O-QUA-SAIP-180920/1687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SAIP-180920/1690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3634**		
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1691
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1692
Buffer Copy without	09-Sep-20	7.2	Out of bound access can happen in MHI command	https://www.qualcomm.	O-QUA-SAIP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	com/company/product-security/bulletins/september-2020-bulletin	180920/1693
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SAIP-180920/1695
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SAIP-180920/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SAIP-180920/1697
ipq6018_firmware					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ6-180920/1698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ6-180920/1699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ6-180920/1700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ6-180920/1701
Buffer Copy	08-Sep-20	10	u'Buffer Overflow in mic	https://ww	O-QUA-IPQ6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/1702
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ6-180920/1703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-IPQ6-180920/1704
Integer Underflow (Wrap or Wraparoun	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE	https://www.qualcomm.com/company/product-	O-QUA-IPQ6-180920/1705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	security/bulletins/august-2020-bulletin	
kamorta_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1709
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1710
Use After	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer	https://www.qualcomm.	O-QUA-KAMO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	com/company/product-security/bulletins/september-2020-bulletin	180920/1711
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-KAMO-180920/1712
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-KAMO-180920/1714
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-KAMO-180920/1720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	-2020-bulletin	
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-KAMO-180920/1721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1722
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1723
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-KAMO-180920/1724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-KAMO-180920/1725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-KAMO-180920/1726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1727
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-KAMO-180920/1730
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-KAMO-180920/1731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**		
bitra_firmware					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-BITR-180920/1732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-BITR-180920/1733
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of	https://www.qualcomm.com/compan	O-QUA-BITR-180920/1734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	y/product-security/bulletins/august-2020-bulletin	
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-BITR-180920/1735

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 APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-BITR-180920/1736
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-BITR-180920/1737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-BITR-180920/1738
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-BITR-180920/1739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-BITR-180920/1740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input	08-Sep-20	4.6	u'Channel name string which has been read from shared	https://www.qualcomm.	O-QUA-BITR-180920/1741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-BITR-180920/1742
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-BITR-180920/1743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-BITR-180920/1744
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-BITR-180920/1745
qcs610_firmware					
Buffer Copy	08-Sep-20	10	u'Possible out of bound write	https://ww	O-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/1746
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	O-QUA-QCS6-180920/1747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	bulletin	
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS6-180920/1748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1749
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in	https://www.qualcomm.com/company/product-security/bulletins/septem	O-QUA-QCS6-180920/1750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	ber-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-QCS6-180920/1756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1757
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCS6-180920/1760
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout	https://www.qualcomm.	O-QUA-QCS6-180920/1761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	com/company/product-security/bulletins/september-2020-bulletin	
sa8155p_firmware					
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SA81-180920/1762
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in	https://www.qualcomm.com/compan	O-QUA-SA81-180920/1763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	y/product-security/bulletins/september-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-SA81-180920/1764
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on	https://www.qualcomm.com/compan	O-QUA-SA81-180920/1765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	y/product-security/bulletins/september-2020-bulletin	
sa515m_firmware					
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA51-180920/1766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA51-180920/1767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA51-180920/1768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-SA51-180920/1769
mdm9645_firmware					
Integer	08-Sep-20	2.1	u'Lack of check of integer	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	MDM9-180920/1770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-MDM9-180920/1773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	O-QUA-MDM9-180920/1774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
qca4531_firmware					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA4-180920/1775
qca9558_firmware					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA9-180920/1776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca6390_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/1777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/1778
Improper Restriction of Operations within the	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-180920/1779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	etins/august-2020-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	O-QUA-QCA6-180920/1780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Redhat					
enterprise_linux					
Use After Free	03-Sep-20	2.1	A use after free was found in igc_reloc_struct_ptr() of psi/igc.c of ghostscript-9.25. A local attacker could supply a specially crafted PDF file to cause a denial of service. **CVE ID : CVE-2020-14373**	N/A	O-RED-ENTE-180920/1781
redlion					
n-tron_702-w_firmware					
Hidden Functionality	01-Sep-20	10	The affected product is vulnerable due to an undocumented interface found on the device, which may allow an attacker to execute commands as root on the device on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16204**	N/A	O-RED-N-TR-180920/1782
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	The affected product is vulnerable to stored cross-site scripting, which may allow an attacker to remotely execute arbitrary code to gain access to sensitive data on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16206**	N/A	O-RED-N-TR-180920/1783
Cross-Site Request Forgery (CSRF)	01-Sep-20	9.3	The affected product is vulnerable to cross-site request forgery, which may allow an attacker to modify different configurations of a	N/A	O-RED-N-TR-180920/1784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device by luring an authenticated user to click on a crafted link on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16208**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	The affected product is vulnerable to reflected cross-site scripting, which may allow an attacker to remotely execute arbitrary code and perform actions in the context of an attacked user on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16210**	N/A	O-RED-N-TR-180920/1785
n-tron_702m12-w_firmware					
Hidden Functionality	01-Sep-20	10	The affected product is vulnerable due to an undocumented interface found on the device, which may allow an attacker to execute commands as root on the device on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16204**	N/A	O-RED-N-TR-180920/1786
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	The affected product is vulnerable to stored cross-site scripting, which may allow an attacker to remotely execute arbitrary code to gain access to sensitive data on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16206**	N/A	O-RED-N-TR-180920/1787
Cross-Site Request Forgery	01-Sep-20	9.3	The affected product is vulnerable to cross-site request forgery, which may	N/A	O-RED-N-TR-180920/1788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			allow an attacker to modify different configurations of a device by luring an authenticated user to click on a crafted link on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16208**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	The affected product is vulnerable to reflected cross-site scripting, which may allow an attacker to remotely execute arbitrary code and perform actions in the context of an attacked user on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16210**	N/A	O-RED-N-TR-180920/1789
Sagemcom					
f\@st_5280_router_firmware					
Deserialization of Untrusted Data	01-Sep-20	9	Sagemcom F@ST 5280 routers using firmware version 1.150.61 have insecure deserialization that allows any authenticated user to perform a privilege escalation to any other user. By making a request with valid sess_id, nonce, and ha1 values inside of the serialized session cookie, an attacker may alter the user value inside of this cookie, and assume the role and permissions of the user specified. By assuming the role of the user internal, which is inaccessible to end users by default, the attacker gains the permissions of the internal	N/A	O-SAG-F\@S-180920/1790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account, which includes the ability to flash custom firmware to the router, allowing the attacker to achieve a complete compromise. **CVE ID : CVE-2020-24034**		
Siemens					
simatic_hmi_comfort_panels_firmware					
Improper Restriction of Excessive Authentication Attempts	09-Sep-20	7.5	A vulnerability has been identified in SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions >= 14 and V < XX), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI Mobile Panels (All versions), SIMATIC HMI United Comfort Panels (All versions). Affected devices insufficiently block excessive authentication attempts. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack. **CVE ID : CVE-2020-15786**	N/A	O-SIE-SIMA-180920/1791
simatic_s7-300_cpu_315f-2_dp_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and	N/A	O-SIE-SIMA-180920/1792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**		
simatic_s7-300_cpu_315f-2_pn_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	O-SIE-SIMA-180920/1793
simatic_s7-300_cpu_317f-2_pn_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password.	N/A	O-SIE-SIMA-180920/1794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**		
simatic_s7-300_cpu_317f-2_dp_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	O-SIE-SIMA-180920/1795
simatic_s7-400_cpu_412_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid	N/A	O-SIE-SIMA-180920/1796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PLC credentials. **CVE ID : CVE-2020-15791**		
simatic_s7-400_cpu_414_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	O-SIE-SIMA-180920/1797
simatic_s7-400_cpu_416_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	O-SIE-SIMA-180920/1798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
simatic_s7-400_cpu_417_firmware					
Insufficientl y Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	O-SIE-SIMA-180920/1799
simatic_s7-300_cpu_314_firmware					
Insufficientl y Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	O-SIE-SIMA-180920/1800
simatic_s7-300_cpu_315-2_dp_firmware					
Insufficientl	09-Sep-20	3.3	A vulnerability has been	N/A	O-SIE-SIMA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
y Protected Credentials			identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**		180920/1801
simatic_hmi_basic_panels_2nd_generation_firmware					
Improper Restriction of Excessive Authentication Attempts	09-Sep-20	7.5	A vulnerability has been identified in SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions >= 14 and V < XX), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI Mobile Panels (All versions), SIMATIC HMI United Comfort Panels (All versions). Affected devices insufficiently block excessive authentication attempts. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack. **CVE ID : CVE-2020-15786**	N/A	O-SIE-SIMA-180920/1802
simatic_hmi_mobile_panels_firmware					
Improper Restriction	09-Sep-20	7.5	A vulnerability has been identified in SIMATIC HMI	N/A	O-SIE-SIMA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Excessive Authentication Attempts			Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions >= 14 and V < XX), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI Mobile Panels (All versions), SIMATIC HMI United Comfort Panels (All versions). Affected devices insufficiently block excessive authentication attempts. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack. **CVE ID : CVE-2020-15786**		180920/1803
simatic_hmi_united_comfort_panels_firmware					
Improper Restriction of Excessive Authentication Attempts	09-Sep-20	7.5	A vulnerability has been identified in SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions >= 14 and V < XX), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI Mobile Panels (All versions), SIMATIC HMI United Comfort Panels (All versions). Affected devices insufficiently block excessive authentication attempts. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack. **CVE ID : CVE-2020-15786**	N/A	O-SIE-SIMA-180920/1804
Improper Authenticat	09-Sep-20	7.5	A vulnerability has been identified in SIMATIC HMI	N/A	O-SIE-SIMA-180920/1805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion			United Comfort Panels (All versions). Affected devices insufficiently validate authentication attempts as the information given can be truncated to match only a set number of characters versus the whole provided string. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack. **CVE ID : CVE-2020-15787**		
simatic_s7-300_cpu_312_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	O-SIE-SIMA-180920/1806
simatic_s7-300_cpu_315-2_pn_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family	N/A	O-SIE-SIMA-180920/1807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**		
simatic_s7-300_cpu_317-2_pn_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	O-SIE-SIMA-180920/1808
simatic_s7-300_cpu_317-2_dp_firmware					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and	N/A	O-SIE-SIMA-180920/1809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**		
Suse					
linux_enterprise_server					
Acceptance of Extraneous Untrusted Data With Trusted Data	01-Sep-20	7.2	A acceptance of Extraneous Untrusted Data With Trusted Data vulnerability in the start script of openldap2 of SUSE Enterprise Storage 5, SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SECURITY, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8,	https://bugzilla.suse.com/show_bug.cgi?id=1172698	O-SUS-LINU-180920/1810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SUSE OpenStack Cloud Crowbar 8; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to escalate privileges from user ldap to root. This issue affects: SUSE Enterprise Storage 5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Debuginfo 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Debuginfo 11-SP4 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Point of Sale 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 11-SECURITY openldap2-client-openssl1 versions prior to 2.4.26-0.74.13.1. SUSE Linux Enterprise Server 11-SP4-LTSS openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 12-SP2-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP2-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP4 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP5		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.31.1. SUSE Linux Enterprise Server for SAP 12-SP2 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 12-SP3 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.31.1. SUSE OpenStack Cloud 7 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud 8 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud Crowbar 8 openldap2 versions prior to 2.4.41-18.71.2. openSUSE Leap 15.1 openldap2 versions prior to 2.4.46-lp151.10.12.1. openSUSE Leap 15.2 openldap2 versions prior to 2.4.46-lp152.14.3.1. **CVE ID : CVE-2020-8023**		
Tendacn					
ac18_firmware					
Improper Authentication	04-Sep-20	6.8	Tenda AC18 Router through V15.03.05.05_EN and through V15.03.05.19(6318) CN devices could cause a remote code execution due to incorrect authentication handling of vulnerable logincheck() function in /usr/lib/lua/ngx_authserver/	N/A	O-TEN-AC18-180920/1811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ngx_wdas.lua file if the administrator UI Interface is set to "radius". **CVE ID : CVE-2020-24987**		
ZTE					
zxr10_2800-4_almpufb\(low\)_firmware					
N/A	01-Sep-20	5	A ZTE product has a DoS vulnerability. Because the equipment couldn't distinguish the attack packets and normal packets with valid http links, the remote attackers could use this vulnerability to cause the equipment WEB/TELNET module denial of service and make the equipment be out of management. This affects: ZXR10 2800-4_ALMPUFB(LOW), all versions up to V3.00.40. **CVE ID : CVE-2020-6873**	N/A	O-ZTE-ZXR1-180920/1812
zxiptv_firmware					
Insufficientl y Protected Credentials	01-Sep-20	5.5	A ZTE product is impacted by the cryptographic issues vulnerability. The encryption algorithm is not properly used, so remote attackers could use this vulnerability for account credential enumeration attack or brute-force attack for password guessing. This affects: ZXIPTV, ZXIPTV-WEB-PV5.09.08.04. **CVE ID : CVE-2020-6874**	N/A	O-ZTE-ZXIP-180920/1813
Zyxel					
vmg5313-b30b_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	02-Sep-20	10	Zyxel VMG5313-B30B router on firmware 5.13(ABCJ.6)b3_1127, and possibly older versions of firmware are affected by insecure permissions which allows regular and other users to create new users with elevated privileges. This is done by changing "FirstIndex" field in JSON that is POST-ed during account creation. Similar may also be possible with account deletion. **CVE ID : CVE-2020-24355**	N/A	O-ZYX-VMG5-180920/1814
Hardware					
Cisco					
email_security_appliance					
Improper Input Validation	04-Sep-20	5	A vulnerability in the web-based management interface of Cisco AsyncOS software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to insufficient validation of requests that are sent to the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the interface of an affected device. A successful exploit could allow the attacker to obtain the IP addresses that are configured on the internal interfaces of the affected	N/A	H-CIS-EMAI-180920/1815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. There is a workaround that addresses this vulnerability. **CVE ID : CVE-2020-3546**		
asr_9000v					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**	N/A	H-CIS-ASR_-180920/1816
asr_9001					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an	N/A	H-CIS-ASR_-180920/1817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
asr_9006					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific	N/A	H-CIS-ASR_-180920/1818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
asr_9010					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability	N/A	H-CIS-ASR_-180920/1819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
asr_9901					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**	N/A	H-CIS-ASR_-180920/1820
asr_9904					
Incorrect Authorizati	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR	N/A	H-CIS-ASR_-180920/1821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
asr_9906					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group	N/A	H-CIS-ASR_-180920/1822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
asr_9910					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to	N/A	H-CIS-ASR_-180920/1823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
asr_9912					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**	N/A	H-CIS-ASR_-180920/1824
asr_9922					
Incorrect Authorizati	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI	N/A	H-CIS-ASR_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		180920/1825
firepower_9300					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.2	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could exploit this vulnerability by supplying a crafted file that,	N/A	H-CIS-FIRE-180920/1826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when it is processed, may cause a stack-based buffer overflow. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An attacker would need to have valid administrative credentials to exploit this vulnerability. **CVE ID : CVE-2020-3545**		
firepower_4115					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.2	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could exploit this vulnerability by supplying a crafted file that, when it is processed, may cause a stack-based buffer overflow. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An attacker would need to have valid administrative credentials to exploit this vulnerability. **CVE ID : CVE-2020-3545**	N/A	H-CIS-FIRE-180920/1827
firepower_4125					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.2	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could exploit this vulnerability by supplying a crafted file that, when it is processed, may cause a stack-based buffer overflow. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An attacker would need to have valid administrative credentials to exploit this vulnerability. **CVE ID : CVE-2020-3545**	N/A	H-CIS-FIRE-180920/1828
firepower_4145					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.2	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could exploit this vulnerability by supplying a crafted file that, when it is processed, may cause a stack-based buffer overflow. A successful exploit	N/A	H-CIS-FIRE-180920/1829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An attacker would need to have valid administrative credentials to exploit this vulnerability. **CVE ID : CVE-2020-3545**		
firepower_4110					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.2	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could exploit this vulnerability by supplying a crafted file that, when it is processed, may cause a stack-based buffer overflow. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An attacker would need to have valid administrative credentials to exploit this vulnerability. **CVE ID : CVE-2020-3545**	N/A	H-CIS-FIRE-180920/1830
firepower_4120					
Improper Restriction of Operations	04-Sep-20	7.2	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative	N/A	H-CIS-FIRE-180920/1831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could exploit this vulnerability by supplying a crafted file that, when it is processed, may cause a stack-based buffer overflow. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An attacker would need to have valid administrative credentials to exploit this vulnerability. **CVE ID : CVE-2020-3545**		
firepower_4140					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.2	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could exploit this vulnerability by supplying a crafted file that, when it is processed, may cause a stack-based buffer overflow. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An	N/A	H-CIS-FIRE-180920/1832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to have valid administrative credentials to exploit this vulnerability. **CVE ID : CVE-2020-3545**		
firepower_4150					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.2	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could exploit this vulnerability by supplying a crafted file that, when it is processed, may cause a stack-based buffer overflow. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An attacker would need to have valid administrative credentials to exploit this vulnerability. **CVE ID : CVE-2020-3545**	N/A	H-CIS-FIRE-180920/1833
rv340w					
Improper Restriction of Operations within the Bounds of a Memory	04-Sep-20	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute	N/A	H-CIS-RV34-180920/1834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3451**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.7	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3453**	N/A	H-CIS-RV34-180920/1835
rv340					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3451**	N/A	H-CIS-RV34-180920/1836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.7	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3453**	N/A	H-CIS-RV34-180920/1837
rv345					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3451**	N/A	H-CIS-RV34-180920/1838
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.7	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute	N/A	H-CIS-RV34-180920/1839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3453**		
rv345p					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3451**	N/A	H-CIS-RV34-180920/1840
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.7	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3453**	N/A	H-CIS-RV34-180920/1841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
8201					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**	N/A	H-CIS-8201-180920/1842
8202					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this	N/A	H-CIS-8202-180920/1843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**		
8808					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**	N/A	H-CIS-8808-180920/1844
8812					
Incorrect Authorizati	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI	N/A	H-CIS-8812-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**		180920/1845
8818					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass	N/A	H-CIS-8818-180920/1846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**		
ios_xrv_9000					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**	N/A	H-CIS-IOS_-180920/1847
ncs_6008					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and	N/A	H-CIS-NCS_-180920/1848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**		
ncs_4009					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform	N/A	H-CIS-NCS_-180920/1849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			actions on the device without authorization checks. **CVE ID : CVE-2020-3473**		
ncs_4016					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**	N/A	H-CIS-NCS_-180920/1850
firepower_4112					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Sep-20	7.2	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could	N/A	H-CIS-FIRE-180920/1851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by supplying a crafted file that, when it is processed, may cause a stack-based buffer overflow. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An attacker would need to have valid administrative credentials to exploit this vulnerability. **CVE ID : CVE-2020-3545**		
ncs_1001					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read	N/A	H-CIS-NCS_-180920/1852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
ncs_1002					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**	N/A	H-CIS-NCS_-180920/1853
ncs_1004					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an	N/A	H-CIS-NCS_-180920/1854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
ncs_5501					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first	N/A	H-CIS-NCS_-180920/1855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**		
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**	N/A	H-CIS-NCS_-180920/1856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ncs_5501-se					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**	N/A	H-CIS-NCS_-180920/1857
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could	N/A	H-CIS-NCS_-180920/1858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
ncs_5502					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**	N/A	H-CIS-NCS_-180920/1859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**	N/A	H-CIS-NCS_-180920/1860
ncs_5502-se					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a	N/A	H-CIS-NCS_-180920/1861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**		
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific	N/A	H-CIS-NCS_-180920/1862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
ncs_5508					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**	N/A	H-CIS-NCS_-180920/1863
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is	N/A	H-CIS-NCS_-180920/1864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
ncs_5516					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform	N/A	H-CIS-NCS_-180920/1865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			actions on the device without authorization checks. **CVE ID : CVE-2020-3473**		
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**	N/A	H-CIS-NCS_-180920/1866
ncs_6000					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and	N/A	H-CIS-NCS_-180920/1867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**		
ncs_5001					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to	N/A	H-CIS-NCS_-180920/1868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**		
ncs_5002					
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**	N/A	H-CIS-NCS_-180920/1869
ncs_5011					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	04-Sep-20	5.6	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges. **CVE ID : CVE-2020-3530**	N/A	H-CIS-NCS_-180920/1870
ncs_540					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a	N/A	H-CIS-NCS_-180920/1871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**		
ncs_560					
Incorrect Authorization	04-Sep-20	7.2	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks. **CVE ID : CVE-2020-3473**	N/A	H-CIS-NCS_-180920/1872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dell					
g7_17_7790					
Use After Free	02-Sep-20	7.2	Dell G7 17 7790 BIOS versions prior to 1.13.2 contain a UEFI BIOS Boot Services overwrite vulnerability. A local attacker with access to system memory may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in System Management Mode (SMM). **CVE ID : CVE-2020-5378**	N/A	H-DEL-G7_1-180920/1873
inspiron_7347					
Use After Free	02-Sep-20	7.2	Dell Inspiron 7347 BIOS versions prior to A13 contain a UEFI BIOS Boot Services overwrite vulnerability. A local attacker with access to system memory may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in System Management Mode (SMM). **CVE ID : CVE-2020-5376**	N/A	H-DEL-INSP-180920/1874
inspiron_7352					
N/A	02-Sep-20	7.2	Dell Inspiron 7352 BIOS versions prior to A12 contain a UEFI BIOS Boot Services overwrite vulnerability. A local attacker with access to system memory may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure	N/A	H-DEL-INSP-180920/1875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary code in System Management Mode (SMM). **CVE ID : CVE-2020-5379**		
Dlink					
dcs-2530l					
N/A	02-Sep-20	9	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. cgi-bin/ddns_enc.cgi allows authenticated command injection. **CVE ID : CVE-2020-25079**	N/A	H-DLI-DCS--180920/1876
dcs-2670l					
N/A	02-Sep-20	9	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. cgi-bin/ddns_enc.cgi allows authenticated command injection. **CVE ID : CVE-2020-25079**	N/A	H-DLI-DCS--180920/1877
D-link					
dcs-2530l					
N/A	02-Sep-20	5	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. The unauthenticated /config/getuser endpoint allows for remote administrator password disclosure. **CVE ID : CVE-2020-25078**	N/A	H-D-L-DCS--180920/1878
dcs-2670l					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Sep-20	5	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. The unauthenticated /config/getuser endpoint allows for remote administrator password disclosure. **CVE ID : CVE-2020-25078**	N/A	H-D-L-DCS--180920/1879
Huawei					
honor_view_20					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);V	N/A	H-HUA-HONO-180920/1880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ersions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
honor_20_pro					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Ve	N/A	H-HUA-HONO-180920/1881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rsions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
oxfords-an00a					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Ver	N/A	H-HUA-OXFO-180920/1882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
b2368-22					
Improper Control of Generation	03-Sep-20	7.7	B2368-22 V100R001C00;B2368-57 V100R001C00;B2368-66	N/A	H-HUA-B236-180920/1883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			V100R001C00 have a command injection vulnerability. An attacker with high privileges may exploit this vulnerability through some operations on the LAN. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject commands to the target device. **CVE ID : CVE-2020-9199**		
b2368-57					
Improper Control of Generation of Code ('Code Injection')	03-Sep-20	7.7	B2368-22 V100R001C00;B2368-57 V100R001C00;B2368-66 V100R001C00 have a command injection vulnerability. An attacker with high privileges may exploit this vulnerability through some operations on the LAN. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject commands to the target device. **CVE ID : CVE-2020-9199**	N/A	H-HUA-B236-180920/1884
b2368-66					
Improper Control of Generation of Code ('Code Injection')	03-Sep-20	7.7	B2368-22 V100R001C00;B2368-57 V100R001C00;B2368-66 V100R001C00 have a command injection vulnerability. An attacker with high privileges may exploit this vulnerability through	N/A	H-HUA-B236-180920/1885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some operations on the LAN. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject commands to the target device. **CVE ID : CVE-2020-9199**		
yale-al00a					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Vers	N/A	H-HUA-YALE-180920/1886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
yale-l21a					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);V	N/A	H-HUA-YALE-180920/1887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ersions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
yale-l61a					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versi	N/A	H-HUA-YALE-180920/1888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ons earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
princeton-al10b					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Vers	N/A	H-HUA-PRIN-180920/1889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
princeton-al10d					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2)	N/A	H-HUA-PRIN-180920/1890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
princeton-tl10c					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Vers	N/A	H-HUA-PRIN-180920/1891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
tony-al00b					
Information Exposure	03-Sep-20	2.1	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);V	N/A	H-HUA-TONY-180920/1892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ersions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak. **CVE ID : CVE-2020-9235**		
mate_20					
Improper Input Validation	03-Sep-20	2.1	HUAWEI Mate 20 smart phones with Versions earlier than 10.1.0.163(C00E160R3P8) have a denial of service (DoS) vulnerability. The attacker can enter a large amount of text on the phone. Due to insufficient verification of the parameter, successful exploitation can impact the service. **CVE ID : CVE-2020-9083**	N/A	H-HUA-MATE-180920/1893
Lenovo					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_x1_carbon_\(20bx\)					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	H-LEN-THIN-180920/1894
thinkpad_t495_drift					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	H-LEN-THIN-180920/1895
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the	N/A	H-LEN-THIN-180920/1896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**		
thinkpad_t495s_jazz					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	H-LEN-THIN-180920/1897
thinkpad_a275					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	H-LEN-THIN-180920/1898
thinkpad_a475					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w;	N/A	H-LEN-THIN-180920/1899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**		
thinkpad_a285					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	H-LEN-THIN-180920/1900
thinkpad_a485					
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	H-LEN-THIN-180920/1901
thinkpad_x395					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Sep-20	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access. **CVE ID : CVE-2020-8335**	N/A	H-LEN-THIN-180920/1902
thinkpad_t490_\(20nx\)					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	H-LEN-THIN-180920/1903
thinkpad_t490_\(20qx\)					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3	N/A	H-LEN-THIN-180920/1904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**		
thinkpad_t490_\(20rx\)					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	H-LEN-THIN-180920/1905
thinkpad_t490s_\(20nx\)					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write	N/A	H-LEN-THIN-180920/1906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**		
thinkpad_t590_\(20nx\)					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	H-LEN-THIN-180920/1907
thinkpad_x1_carbon_\(20qx\)					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	H-LEN-THIN-180920/1908
thinkpad_x1_yoga_\(20qx\)					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	H-LEN-THIN-180920/1909
thinkpad_x390_\(20qx\)					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**	N/A	H-LEN-THIN-180920/1910
thinkpad_x390_\(20sx\)					
N/A	01-Sep-20	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer	N/A	H-LEN-THIN-180920/1911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2020-8341**		
Netgear					
r8300					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Sep-20	5.8	NETGEAR R8300 devices before 1.0.2.134 are affected by command injection by an unauthenticated attacker. **CVE ID : CVE-2020-25067**	N/A	H-NET-R830-180920/1912
Philips					
intellivue_mp2-mp90					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the	N/A	H-PHI-INTE-180920/1913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	H-PHI-INTE-180920/1914
intellivue_mx100					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart.	N/A	H-PHI-INTE-180920/1915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16216		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	H-PHI-INTE-180920/1916
intellivue_mx400					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	H-PHI-INTE-180920/1917
Improper Check for Certificate	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue	N/A	H-PHI-INTE-180920/1918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Revocation			patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**		
intellivue_mx850					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	H-PHI-INTE-180920/1919
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software	N/A	H-PHI-INTE-180920/1920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**		
intellivue_x2					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	H-PHI-INTE-180920/1921
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate.	N/A	H-PHI-INTE-180920/1922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16228		
intellivue_x3					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	H-PHI-INTE-180920/1923
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	H-PHI-INTE-180920/1924
intellivue_mx800					
Improper Input	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02,	N/A	H-PHI-INTE-180920/1925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	H-PHI-INTE-180920/1926
intellivue_mx750					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior,	N/A	H-PHI-INTE-180920/1927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	H-PHI-INTE-180920/1928
intellivue_mx700					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the	N/A	H-PHI-INTE-180920/1929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	H-PHI-INTE-180920/1930
intellivue_mx600					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart.	N/A	H-PHI-INTE-180920/1931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16216		
Improper Check for Certificate Revocation	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**	N/A	H-PHI-INTE-180920/1932
intellivue_mx550					
Improper Input Validation	11-Sep-20	6.1	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart. **CVE ID : CVE-2020-16216**	N/A	H-PHI-INTE-180920/1933
Improper Check for Certificate	11-Sep-20	5.2	Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, PerformanceBridge Focal Point Version A.01, IntelliVue	N/A	H-PHI-INTE-180920/1934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Revocation			patient monitors MX100, MX400-MX850, and MP2-MP90 Versions N and prior, IntelliVue X3 and X2 Versions N and prior. The software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate. **CVE ID : CVE-2020-16228**		
Qualcomm					
mdm9206					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1937
Time-of-check	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during	https://www.qualcomm.	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	com/company/product-security/bulletins/august-2020-bulletin	180920/1938
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than	https://www.qualcomm.com/company/product-	H-QUA-MDM9-180920/1940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MDM9-180920/1943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1945
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
mdm9607					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MDM9-180920/1950
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MDM9-180920/1957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1960
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MDM9-180920/1961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/1962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
msm8909w					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1963
Buffer Copy without Checking Size of Input	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-MSM8-180920/1964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	etins/august-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MSM8-180920/1967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1968
Improper Input Validation	08-Sep-20	4.6	u'Possible out of bound write in DSP driver code due to lack of check of data received from user' in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-180920/1969

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 MSM8909W **CVE ID : CVE-2020-3648**	security/bulletins/august-2020-bulletin	
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1970
msm8996au					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-MSM8-180920/1971

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 APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-MSM8-180920/1975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**	bulletin	
Integer	08-Sep-20	4.6	u'A potential buffer overflow	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	MSM8-180920/1976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MSM8-180920/1977
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-MSM8-180920/1978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/1981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**		
qca6574au					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA6-180920/1982
Buffer Copy without	08-Sep-20	10	u'Possible out of bound write while processing association	https://www.qualcomm.	H-QUA-QCA6-180920/1983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	com/company/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA6-180920/1984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA6-180920/1985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qcs405					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1989
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS4-180920/1990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1991
Integer Overflow or Wraparoun	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read	https://www.qualcomm.com/compan	H-QUA-QCS4-180920/1992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d			from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	y/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1997
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/1998
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS4-180920/1999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2001
Buffer Copy without Checking Size of Input	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS4-180920/2002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	etins/august-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS4-180920/2004
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2006
qcs605					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2010
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer	https://www.qualcomm.com/company/product-	H-QUA-QCS6-180920/2011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	security/bulletins/august-2020-bulletin	
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS6-180920/2012
Buffer Copy without Checking Size of Input	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS6-180920/2013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	etins/august-2020-bulletin	
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS6-180920/2014
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SXR1130 **CVE ID : CVE-2020-3611**		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS6-180920/2016
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-	H-QUA-QCS6-180920/2022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2025
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS6-180920/2026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2028
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-QCS6-180920/2029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
sda660					
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA6-180920/2031
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDA6-180920/2032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3617		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA6-180920/2033
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SDA6-180920/2034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**	-2020-bulletin	
Improper	08-Sep-20	4.9	u'Lack of check to ensure that	https://ww	H-QUA-SDA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA6-180920/2036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA6-180920/2037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDA6-180920/2038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA6-180920/2039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3643		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA6-180920/2040
sdm439					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SDM4-180920/2041

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 APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11120		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2045
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM4-180920/2046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM4-180920/2052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM4-180920/2054
sdm630					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2057
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-	H-QUA-SDM6-180920/2058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	bulletin	
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2059
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2061
Integer	08-Sep-20	2.1	u'Lack of check of integer	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	SDM6-180920/2062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2068
Out-of-bounds	08-Sep-20	7.2	u'Out of bounds memory access during memory copy	https://www.qualcomm.	H-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	com/company/product-security/bulletins/august-2020-bulletin	180920/2069
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SDM6-180920/2070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
sdm660					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11115		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2073
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDM6-180920/2074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	etins/august-2020-bulletin	
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2076
Buffer Copy without Checking Size of	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-SDM6-180920/2077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	security/bulletins/august-2020-bulletin	
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2078
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2080
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/septem	H-QUA-SDM6-180920/2086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	ber-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2090
Improper Restriction of Operations within the	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDM6-180920/2091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	etins/august-2020-bulletin	
sdx20					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDX2-180920/2099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2101
mdm9150					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header	https://www.qualcomm.	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	com/company/product-security/bulletins/august-2020-bulletin	180920/2102
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-MDM9-180920/2103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/septem	H-QUA-MDM9-180920/2109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	ber-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
mdm9640					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2114
Integer Overflow or	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round	https://www.qualcomm.	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	com/company/product-security/bulletins/august-2020-bulletin	180920/2115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MDM9-180920/2119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
mdm9650					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2122
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-MDM9-180920/2123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	-2020-bulletin	
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MDM9-180920/2130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
sdx24					
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2134
Time-of-check Time-of-use (TOCTOU) Race	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDX2-180920/2135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition			corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	etins/august-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage'	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SDX2-180920/2137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**	bulletin	
Improper	08-Sep-20	4.6	u'Channel name string which	https://ww	H-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDX2-180920/2140
Information	08-Sep-20	2.1	u'Information disclosure issue	https://ww	H-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2141
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating	https://www.qualcomm.com/company/product-	H-QUA-SDX2-180920/2142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX2-180920/2144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3666		
ipq4019					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ4-180920/2145
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ4-180920/2146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ4-180920/2147
ipq8064					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2148
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2150
ipq8074					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug	https://www.qualcomm.com/compan	H-QUA-IPQ8-180920/2151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	y/product-security/bulletins/august-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2158
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ8-180920/2160
qca6174a					
Out-of-	08-Sep-20	5	u'Buffer over read occurs	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2161
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-QCA6-180920/2162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA6-180920/2163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA6-180920/2164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca9377					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-11118**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2168
qca9379					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2169
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-QCA9-180920/2170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
sdm429w					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2176
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from	https://www.qualcomm.com/compan	H-QUA-SDM4-180920/2178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	y/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM4-180920/2181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2183
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM4-180920/2184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sc7180					
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SC71-180920/2185
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SC71-180920/2192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2193
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2194
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SC71-180920/2195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2198
Improper Restriction of Operations within the Bounds of a Memory	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SC71-180920/2199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC71-180920/2200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3675		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SC71-180920/2201
apq8009					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2205
Time-of-check Time-of-use (TOCTOU) Race	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory	https://www.qualcomm.com/company/product-security/bull	H-QUA-APQ8-180920/2206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition			corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	etins/august-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage'	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-APQ8-180920/2208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**	bulletin	
Improper	08-Sep-20	4.6	u'Channel name string which	https://ww	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2212
Buffer Copy without Checking Size of	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value	https://www.qualcomm.com/company/product-	H-QUA-APQ8-180920/2213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	security/bulletins/september-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
apq8098					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2217
Use After	08-Sep-20	4.6	u'Calling thread may free the	https://ww	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2218
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2219
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-APQ8-180920/2220

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 APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	etins/august-2020-bulletin	
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-APQ8-180920/2221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11135		
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2222
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-APQ8-180920/2228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2232
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
msm8953					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2237
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MSM8-180920/2239
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2242

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string	https://www.qualcomm.com/company/product-	H-QUA-MSM8-180920/2243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MSM8-180920/2245
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-	https://www.qualcomm.com/compan	H-QUA-MSM8-180920/2246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	y/product-security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/septem	H-QUA-MSM8-180920/2247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	ber-2020-bulletin	
msm8998					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2250
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2252
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3619		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MSM8-180920/2259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3644		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2262
Buffer Copy without Checking	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer	https://www.qualcomm.com/compan	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	y/product-security/bulletins/august-2020-bulletin	180920/2263
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
nicobar					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-NICO-180920/2265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-NICO-180920/2266
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-NICO-180920/2267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-NICO-180920/2268
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-NICO-180920/2269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-NICO-180920/2270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-NICO-180920/2271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-NICO-180920/2272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	-2020-bulletin	
Integer Underflow (Wrap or	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic	https://www.qualcomm.com/compan	H-QUA-NICO-180920/2273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	y/product-security/bulletins/september-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-NICO-180920/2274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-NICO-180920/2275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-NICO-180920/2276
Buffer Copy	08-Sep-20	10	u'Buffer Overflow in mic	https://ww	H-QUA-NICO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2277
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-NICO-180920/2278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-NICO-180920/2279
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-NICO-180920/2280

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 Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	security/bulletins/september-2020-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-NICO-180920/2281
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-	H-QUA-NICO-180920/2282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	bulletin	
apq8053					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2285
Time-of-check	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during	https://www.qualcomm.	H-QUA-APQ8-180920/2286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	com/company/product-security/bulletins/august-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than	https://www.qualcomm.com/company/product-	H-QUA-APQ8-180920/2288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-APQ8-180920/2291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2293
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper	https://www.qualcomm.com/company/product-	H-QUA-APQ8-180920/2294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	security/bulletins/august-2020-bulletin	
mdm9207c					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
msm8905					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2300
Buffer Copy	08-Sep-20	10	u'Possible out of bound write	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	MSM8-180920/2301
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-MSM8-180920/2302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' 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/august-2020-bulletin	H-QUA-MSM8-180920/2305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow	https://www.qualcomm.	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	com/company/product-security/bulletins/august-2020-bulletin	180920/2307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3624		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MSM8-180920/2308
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-MSM8-180920/2309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
qcn7605					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN7-180920/2311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN7-180920/2312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN7-180920/2313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN7-180920/2314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN7-180920/2315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN7-180920/2316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN7-180920/2317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN7-180920/2318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN7-180920/2319
Integer Underflow (Wrap or Wraparoun	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE	https://www.qualcomm.com/company/product-	H-QUA-QCN7-180920/2320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	security/bulletins/august-2020-bulletin	
sdm845					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2324
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**		
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2326
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SDM8-180920/2332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	-2020-bulletin	
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM8-180920/2333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2335
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM8-180920/2336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2338
Buffer Copy without Checking Size of Input	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDM8-180920/2339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	etins/august-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
apq8076					
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
ipq5018					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ5-180920/2342
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ5-180920/2343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ5-180920/2344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
apq8017					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2345
Time-of-check Time-of-use (TOCTOU)	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege	https://www.qualcomm.com/company/product-	H-QUA-APQ8-180920/2346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Race Condition			escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	security/bulletins/august-2020-bulletin	
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-APQ8-180920/2348

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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	etins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure	https://www.qualcomm.	H-QUA-APQ8-180920/2349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	com/company/product-security/bulletins/august-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-APQ8-180920/2350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	etins/august-2020-bulletin	
apq8096au					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-APQ8-180920/2351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2354
Improper	08-Sep-20	7.2	u'Possible out of bound access	https://ww	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2355
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input	08-Sep-20	4.6	u'Channel name string which has been read from shared	https://www.qualcomm.	H-QUA-APQ8-180920/2358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-APQ8-180920/2360
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure	https://www.qualcomm.	H-QUA-APQ8-180920/2361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	com/company/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-APQ8-180920/2362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	etins/august-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-APQ8-180920/2363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
sda845					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2366
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3611		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2368
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SDA8-180920/2369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**	-2020-bulletin	
Improper	08-Sep-20	4.9	u'Lack of check to ensure that	https://ww	H-QUA-SDA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDA8-180920/2373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3643		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2375
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SDA8-180920/2376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2378
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDA8-180920/2380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
sdm636					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2381
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header	https://www.qualcomm.	H-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	com/company/product-security/bulletins/august-2020-bulletin	180920/2382
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SDM6-180920/2383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	bulletin	
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2384
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2386
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2396
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
sdm670					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11128		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2400
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2401
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2403
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage	https://www.qualcomm.com/company/product-	H-QUA-SDM6-180920/2408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	security/bulletins/august-2020-bulletin	
Integer	09-Sep-20	9.4	u'Multiple Read overflows	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	w.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	SDM6-180920/2409
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2414
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
sdm710					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2417
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail	https://www.qualcomm.com/company/product-	H-QUA-SDM7-180920/2418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	security/bulletins/september-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2419
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM7-180920/2420
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access	https://www.qualcomm.com/company/product-	H-QUA-SDM7-180920/2421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	security/bulletins/august-2020-bulletin	
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM7-180920/2422
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2425

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDM7-180920/2426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	etins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3622		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM7-180920/2428
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SDM7-180920/2429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SDM7-180920/2430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM7-180920/2431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2433
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM7-180920/2435

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6574					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA6-180920/2436
qca8081					
Time-of-	08-Sep-20	6.9	u'Non-secure memory is	https://ww	H-QUA-QCA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
check Time-of-use (TOCTOU) Race Condition			touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2437
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA8-180920/2438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from	https://www.qualcomm.com/compan	H-QUA-QCA8-180920/2439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	y/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA8-180920/2440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA8-180920/2441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA8-180920/2442
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA8-180920/2443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA8-180920/2444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3669		
qcs404					
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS4-180920/2445
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2446
Time-of-check Time-of-use	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution	https://www.qualcomm.com/compan	H-QUA-QCS4-180920/2447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	y/product-security/bulletins/august-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS4-180920/2449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	etins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3621		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2451
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3640		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2453
Information	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic	https://www.qualcomm.	H-QUA-QCS4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	com/company/product-security/bulletins/august-2020-bulletin	180920/2454
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2457
Improper Restriction of Operations	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCS4-180920/2458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	security/bulletins/august-2020-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS4-180920/2459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS4-180920/2460
sxr1130					
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR1-180920/2461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR1-180920/2462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR1-180920/2463
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SXR1-180920/2464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR1-180920/2465
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SXR1-180920/2466
Time-of-check Time-of-use (TOCTOU) Race	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory	https://www.qualcomm.com/company/product-security/bull	H-QUA-SXR1-180920/2467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition			corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	etins/august-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR1-180920/2468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage'	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SXR1-180920/2469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**	bulletin	
Improper	08-Sep-20	4.6	u'Channel name string which	https://ww	H-QUA-SXR1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR1-180920/2471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SXR1-180920/2472
Information	08-Sep-20	2.1	u'Information disclosure issue	https://ww	H-QUA-SXR1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2473
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating	https://www.qualcomm.com/company/product-	H-QUA-SXR1-180920/2474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	security/bulletins/august-2020-bulletin	
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR1-180920/2475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR1-180920/2476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR1-180920/2477
Improper Restriction of Operations within the Bounds of a	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SXR1-180920/2478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	-2020-bulletin	
sm6150					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2482
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM61-180920/2484
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM61-180920/2486
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM61-180920/2487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2488
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SM61-180920/2489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**	bulletin	
Improper Restriction	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write	https://www.qualcomm.	H-QUA-SM61-180920/2490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	com/company/product-security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2493
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM61-180920/2494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2495
Incorrect Calculation of Buffer	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function	https://www.qualcomm.com/compan	H-QUA-SM61-180920/2496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size			exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	y/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2499
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2500
Buffer Copy without Checking Size of Input ('Classic Buffer	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-	H-QUA-SM61-180920/2501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2503
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2505
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in	https://www.qualcomm.com/company/product-security/bulletins/septem	H-QUA-SM61-180920/2506

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 Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	ber-2020-bulletin	
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM61-180920/2507
sm8150					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2508
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SM81-180920/2509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2512
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM81-180920/2513
Improper Validation of Array	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer	https://www.qualcomm.com/company/product-	H-QUA-SM81-180920/2514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Index			size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	security/bulletins/august-2020-bulletin	
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM81-180920/2515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11135		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM81-180920/2516
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM81-180920/2523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2524
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is	https://www.qualcomm.com/compan	H-QUA-SM81-180920/2525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	y/product-security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**		
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2527
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM81-180920/2528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2529
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2531
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to	https://www.qualcomm.com/compan	H-QUA-SM81-180920/2532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	y/product-security/bulletins/september-2020-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM81-180920/2533
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in	https://www.qualcomm.com/company/product-security/bulletins/septem	H-QUA-SM81-180920/2534

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 Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	ber-2020-bulletin	
mdm9615					
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
mdm9625					
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MDM9-180920/2537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
mdm9205					
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/septem	H-QUA-MDM9-180920/2542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	ber-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
msm8909					
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
mdm9655					
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-MDM9-180920/2555

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	bulletin	
Integer Underflow (Wrap or Wraparoun	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in	https://www.qualcomm.com/company/product-	H-QUA-MDM9-180920/2556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	security/bulletins/september-2020-bulletin	
mdm9635m					
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MDM9-180920/2558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
qca6584au					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA6-180920/2559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca9531					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2560
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCA9-180920/2561

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 Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**	security/bulletins/august-2020-bulletin	
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**		
qca9880					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca9886					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca9980					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2565
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qcn5502					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN5-180920/2567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN5-180920/2568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**		
qm215					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QM21-180920/2569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QM21-180920/2570
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-QM21-180920/2571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	-2020-bulletin	
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QM21-180920/2572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QM21-180920/2573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11128		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QM21-180920/2574
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QM21-180920/2575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QM21-180920/2576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QM21-180920/2577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QM21-180920/2578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QM21-180920/2579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QM21-180920/2580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QM21-180920/2581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QM21-180920/2582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3656		
sm7150					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2583
Buffer Copy without Checking	08-Sep-20	10	u'Possible out of bound write while processing association response received from host	https://www.qualcomm.com/compan	H-QUA-SM71-180920/2584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	y/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2587
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM71-180920/2588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2589
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM71-180920/2590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM71-180920/2591
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SM71-180920/2596

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	bulletin	
Buffer Copy without Checking Size of	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on	https://www.qualcomm.com/company/product-	H-QUA-SM71-180920/2597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	security/bulletins/august-2020-bulletin	
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM71-180920/2598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2599
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2600
Information	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure	https://www.qualcomm.	H-QUA-SM71-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	com/company/product-security/bulletins/august-2020-bulletin	180920/2601
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM71-180920/2602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	etins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**		
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2604
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM71-180920/2605
Buffer Copy without Checking	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer	https://www.qualcomm.com/compan	H-QUA-SM71-180920/2606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	y/product-security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM71-180920/2608
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SM71-180920/2609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	-2020-bulletin	
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM71-180920/2610
N/A	08-Sep-20	5	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN	https://www.qualcomm.com/compan	H-QUA-SM71-180920/2611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 **CVE ID : CVE-2020-3702**	y/product-security/bulletins/august-2020-bulletin	
sdm429					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2615
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM4-180920/2617
Time-of-check Time-of-use (TOCTOU) Race	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDM4-180920/2618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition			corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	etins/august-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage'	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SDM4-180920/2620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**	bulletin	
Improper	08-Sep-20	4.6	u'Channel name string which	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	SDM4-180920/2621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM4-180920/2623
Information	08-Sep-20	2.1	u'Information disclosure issue	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	SDM4-180920/2624
Buffer Copy without Checking Size of	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value	https://www.qualcomm.com/company/product-	H-QUA-SDM4-180920/2625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	security/bulletins/september-2020-bulletin	
sdm632					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2629
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2631
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2634

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string	https://www.qualcomm.com/company/product-	H-QUA-SDM6-180920/2635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM6-180920/2636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM6-180920/2637
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-	https://www.qualcomm.com/compan	H-QUA-SDM6-180920/2638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	y/product-security/bulletins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/septem	H-QUA-SDM6-180920/2639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	ber-2020-bulletin	
msm8917					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11118		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2643
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MSM8-180920/2645
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-MSM8-180920/2649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**	-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MSM8-180920/2651
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-MSM8-180920/2652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MSM8-180920/2653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
msm8920					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2656
Improper Validation	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file	https://www.qualcomm.	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Array Index			content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	com/company/product-security/bulletins/august-2020-bulletin	180920/2657
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage	https://www.qualcomm.com/company/product-	H-QUA-MSM8-180920/2662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	security/bulletins/august-2020-bulletin	
Information	08-Sep-20	2.1	u'Information disclosure issue	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	MSM8-180920/2663
msm8937					
Out-of-bounds	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to	https://www.qualcomm.com/compan	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	y/product-security/bulletins/august-2020-bulletin	180920/2664
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3619		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
msm8940					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-11118**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2677
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2680

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not	https://www.qualcomm.com/company/product-security/bull	H-QUA-MSM8-180920/2681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	etins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3622		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3643		
msm8996					
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MSM8-180920/2688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
sdm450					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2690
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of	https://www.qualcomm.com/compan	H-QUA-SDM4-180920/2691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	y/product-security/bulletins/august-2020-bulletin	
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2692

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 APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM4-180920/2694
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/septem	H-QUA-SDM4-180920/2700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	ber-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM4-180920/2701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM4-180920/2702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
sm8250					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2704
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SM82-180920/2705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	-2020-bulletin	
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2707
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM82-180920/2708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-11124**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2709
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM82-180920/2710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11129		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM82-180920/2711
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Buffer Copy without Checking Size of Input	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM82-180920/2715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	etins/august-2020-bulletin	
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2716
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2719
Buffer Copy without Checking Size of Input	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM82-180920/2720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	etins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM82-180920/2721
Buffer Copy without Checking Size of Input	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM82-180920/2722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	etins/august-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM82-180920/2724
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SM82-180920/2725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SM82-180920/2726
sxr2130					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2730
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SXR2-180920/2732
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SXR2-180920/2734
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SXR2-180920/2735
Integer Overflow or	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round	https://www.qualcomm.	H-QUA-SXR2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	com/company/product-security/bulletins/august-2020-bulletin	180920/2736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2739
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**		
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2741
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SXR2-180920/2744
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SXR2-180920/2745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SXR2-180920/2746
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SXR2-180920/2747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**		
qca9563					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qcn5500					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCN5-180920/2749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
sa6155p					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA61-180920/2750
Improper	08-Sep-20	4.3	u'Null Pointer exception while	https://ww	H-QUA-SA61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	180920/2751
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SA61-180920/2752
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA61-180920/2753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SA61-180920/2754
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA61-180920/2755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**	etins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA61-180920/2756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA61-180920/2757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA61-180920/2758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA61-180920/2759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SA61-180920/2760
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA61-180920/2761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SA61-180920/2762
sc8180x					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2763
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SC81-180920/2764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SC81-180920/2766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11124		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2767
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SC81-180920/2769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**	-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2773
Buffer Copy without Checking	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer	https://www.qualcomm.com/compan	H-QUA-SC81-180920/2774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	y/product-security/bulletins/august-2020-bulletin	
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2775
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SC81-180920/2776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2777
Buffer Copy without Checking Size of Input ('Classic	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SC81-180920/2778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SC81-180920/2780
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SC81-180920/2781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SC81-180920/2782
sdm850					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-11133**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2783
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments	https://www.qualcomm.com/compan	H-QUA-SDM8-180920/2784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	y/product-security/bulletins/august-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDM8-180920/2790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2794
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDM8-180920/2796

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcm2150					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCM2-180920/2797
Buffer Copy without Checking Size of Input	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCM2-180920/2798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	etins/august-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCM2-180920/2799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCM2-180920/2800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCM2-180920/2801
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCM2-180920/2802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	security/bulletins/september-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCM2-180920/2803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCM2-180920/2804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCM2-180920/2805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCM2-180920/2806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-	H-QUA-QCM2-180920/2807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCM2-180920/2808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCM2-180920/2809
Buffer Copy	09-Sep-20	7.2	Out of bound access can	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	w.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	QCM2-180920/2810
sdx55					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDX5-180920/2814
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDX5-180920/2820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2821
Incorrect Calculation	08-Sep-20	7.2	u'Resizing the usage table header before passing all the	https://www.qualcomm.	H-QUA-SDX5-180920/2822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Buffer Size			checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	com/company/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2825
Out-of-bounds Write	08-Sep-20	4.6	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3647**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2826
Buffer Copy without Checking Size of Input ('Classic Buffer	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2020-	H-QUA-SDX5-180920/2827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	bulletin	
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDX5-180920/2828
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SDX5-180920/2829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SDX5-180920/2830
rennell					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-RENN-180920/2831

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 APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-RENN-180920/2834
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-RENN-180920/2836
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-RENN-180920/2837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3619		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2843
Integer	09-Sep-20	9.4	u'Multiple Read overflows	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	w.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	RENN-180920/2844
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**		
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2846
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-RENN-180920/2849
Buffer Copy without Checking Size of Input	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-RENN-180920/2850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	etins/august-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2852
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-RENN-180920/2853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-RENN-180920/2854
sa415m					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received	https://www.qualcomm.com/company/product-	H-QUA-SA41-180920/2855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	security/bulletins/august-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA41-180920/2856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**		
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA41-180920/2857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA41-180920/2858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SA41-180920/2859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**	-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA41-180920/2860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SA41-180920/2861
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SA41-180920/2862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA41-180920/2863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA41-180920/2864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA41-180920/2865
Improper Restriction of Operations within the Bounds of a Memory	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SA41-180920/2866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA41-180920/2867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3675		
saipan					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2868
Buffer Copy without Checking	08-Sep-20	10	u'Possible out of bound write while processing association response received from host	https://www.qualcomm.com/compan	H-QUA-SAIP-180920/2869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	y/product-security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2872
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SAIP-180920/2873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2874
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SAIP-180920/2875
Reachable	09-Sep-20	7.8	u'Reachable assertion when	https://ww	H-QUA-SAIP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	w.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	180920/2876
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SAIP-180920/2880

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	bulletin	
Integer Underflow (Wrap or Wraparoun	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in	https://www.qualcomm.com/company/product-	H-QUA-SAIP-180920/2881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	security/bulletins/september-2020-bulletin	
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2883
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SAIP-180920/2884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2885
Information Exposure	09-Sep-20	2.1	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SAIP-180920/2886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3674**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SAIP-180920/2887
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SAIP-180920/2888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**		
ipq6018					
Improper Input Validation	08-Sep-20	7.5	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ6-180920/2889
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ6-180920/2890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ6-180920/2891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ6-180920/2892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ6-180920/2893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ6-180920/2894
Improper Restriction of Operations within the	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ6-180920/2895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	etins/august-2020-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-IPQ6-180920/2896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
kamorta					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2897
Buffer Copy	08-Sep-20	10	u'Possible out of bound write	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**	w.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	KAMO-180920/2898
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-KAMO-180920/2899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**	bulletin	
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11120**		
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2901
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-KAMO-180920/2902
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/septem	H-QUA-KAMO-180920/2903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11135**	ber-2020-bulletin	
Improper Input Validation	08-Sep-20	4.6	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130 **CVE ID : CVE-2020-3611**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2904
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-KAMO-180920/2905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2911
Integer Underflow (Wrap or	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic	https://www.qualcomm.com/compan	H-QUA-KAMO-180920/2912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	y/product-security/bulletins/september-2020-bulletin	
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**		
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2914
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**		
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-KAMO-180920/2917
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-KAMO-180920/2918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2920
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-KAMO-180920/2921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-KAMO-180920/2922
bitra					
Out-of-bounds Read	08-Sep-20	5	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-BITR-180920/2923

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 APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11115**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	08-Sep-20	4.6	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11120		
Improper Input Validation	08-Sep-20	4.3	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11122**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2927
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-11128**		
Use After Free	09-Sep-20	7.2	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130 **CVE ID : CVE-2020-11129**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-BITR-180920/2929
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3629**		
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2934
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	4.6	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-BITR-180920/2935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3646**		
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-BITR-180920/2936
qcs610					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11116**		
Information Exposure	08-Sep-20	5	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11118**		
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS6-180920/2939
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**		
Out-of-bounds Read	09-Sep-20	6.6	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3617**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS6-180920/2941
Time-of-check	08-Sep-20	6.9	u'Non-secure memory is touched multiple times during	https://www.qualcomm.	H-QUA-QCS6-180920/2942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3619**	com/company/product-security/bulletins/august-2020-bulletin	
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than	https://www.qualcomm.com/company/product-	H-QUA-QCS6-180920/2944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS6-180920/2947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3634**		
N/A	08-Sep-20	4.6	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3636**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2948
Incorrect Calculation of Buffer Size	08-Sep-20	7.2	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 **CVE ID : CVE-2020-3640**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCS6-180920/2949
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCS6-180920/2950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-QCS6-180920/2951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	bulletin	
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-QCS6-180920/2952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**		
sa8155p					
Use After Free	09-Sep-20	7.2	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-11124**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SA81-180920/2953
Reachable Assertion	09-Sep-20	7.8	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SA81-180920/2954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11135		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Sep-20	7.2	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3656**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SA81-180920/2955
Information Exposure	09-Sep-20	2.1	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-SA81-180920/2956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3679**		
sa515m					
Improper Validation of Array Index	08-Sep-20	7.2	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-11128**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-SA51-180920/2957
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SA51-180920/2958

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**	bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SA51-180920/2959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3643**	security/bulletins/august-2020-bulletin	
Information Exposure	08-Sep-20	2.1	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-	H-QUA-SA51-180920/2960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3644**	bulletin	
mdm9645					
Integer Overflow or Wraparound	08-Sep-20	2.1	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3620**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	4.9	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2962

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, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3621**		
Improper Input Validation	08-Sep-20	4.6	u'Channel name string which has been read from shared memory is potentially subjected to string	https://www.qualcomm.com/company/product-	H-QUA-MDM9-180920/2963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	security/bulletins/august-2020-bulletin	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3622**		
Integer Overflow or Wraparound	08-Sep-20	4.6	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-MDM9-180920/2964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3624**		
Integer Underflow (Wrap or Wraparound)	09-Sep-20	9.4	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3634**	https://www.qualcomm.com/company/product-security/bulletins/september-2020-bulletin	H-QUA-MDM9-180920/2965
qca4531					
Improper Input	08-Sep-20	7.5	u'In the lbd service, an external user can issue a	https://www.qualcomm.	H-QUA-QCA4-180920/2966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980 **CVE ID : CVE-2020-11117**	com/company/product-security/bulletins/august-2020-bulletin	
qca9558					
Out-of-bounds Write	08-Sep-20	7.2	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA9-180920/2967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130 **CVE ID : CVE-2020-3666**		
qca6390					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-20	10	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3667**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA6-180920/2968
Buffer Copy without Checking	08-Sep-20	10	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length	https://www.qualcomm.com/compan	H-QUA-QCA6-180920/2969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3668**	y/product-security/bulletins/august-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-20	10	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA6-180920/2970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130 **CVE ID : CVE-2020-3669**		
Integer Underflow (Wrap or Wraparound)	08-Sep-20	10	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250 **CVE ID : CVE-2020-3675**	https://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin	H-QUA-QCA6-180920/2971
redlion					
n-tron_702-w					
Hidden Functionality	01-Sep-20	10	The affected product is vulnerable due to an undocumented interface found on the device, which may allow an attacker to execute commands as root on the device on the N-Tron 702-	N/A	H-RED-N-TR-180920/2972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			W / 702M12-W (all versions). **CVE ID : CVE-2020-16204**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	The affected product is vulnerable to stored cross-site scripting, which may allow an attacker to remotely execute arbitrary code to gain access to sensitive data on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16206**	N/A	H-RED-N-TR-180920/2973
Cross-Site Request Forgery (CSRF)	01-Sep-20	9.3	The affected product is vulnerable to cross-site request forgery, which may allow an attacker to modify different configurations of a device by luring an authenticated user to click on a crafted link on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16208**	N/A	H-RED-N-TR-180920/2974
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	The affected product is vulnerable to reflected cross-site scripting, which may allow an attacker to remotely execute arbitrary code and perform actions in the context of an attacked user on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16210**	N/A	H-RED-N-TR-180920/2975
n-tron_702m12-w					
Hidden Functionality	01-Sep-20	10	The affected product is vulnerable due to an undocumented interface found on the device, which may allow an attacker to	N/A	H-RED-N-TR-180920/2976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute commands as root on the device on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16204**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	The affected product is vulnerable to stored cross-site scripting, which may allow an attacker to remotely execute arbitrary code to gain access to sensitive data on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16206**	N/A	H-RED-N-TR-180920/2977
Cross-Site Request Forgery (CSRF)	01-Sep-20	9.3	The affected product is vulnerable to cross-site request forgery, which may allow an attacker to modify different configurations of a device by luring an authenticated user to click on a crafted link on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16208**	N/A	H-RED-N-TR-180920/2978
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-20	3.5	The affected product is vulnerable to reflected cross-site scripting, which may allow an attacker to remotely execute arbitrary code and perform actions in the context of an attacked user on the N-Tron 702-W / 702M12-W (all versions). **CVE ID : CVE-2020-16210**	N/A	H-RED-N-TR-180920/2979
Sagemcom					
f\@st_5280_router					
Deserializat	01-Sep-20	9	Sagemcom F@ST 5280 routers	N/A	H-SAG-F\@S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion of Untrusted Data			using firmware version 1.150.61 have insecure deserialization that allows any authenticated user to perform a privilege escalation to any other user. By making a request with valid sess_id, nonce, and ha1 values inside of the serialized session cookie, an attacker may alter the user value inside of this cookie, and assume the role and permissions of the user specified. By assuming the role of the user internal, which is inaccessible to end users by default, the attacker gains the permissions of the internal account, which includes the ability to flash custom firmware to the router, allowing the attacker to achieve a complete compromise. **CVE ID : CVE-2020-24034**		180920/2980
Siemens					
simatic_s7-300_cpu_315f-2_dp					
Insufficientl y Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password.	N/A	H-SIE-SIMA-180920/2981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**		
simatic_s7-300_cpu_315f-2_pn					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	H-SIE-SIMA-180920/2982
simatic_s7-300_cpu_317f-2_pn					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid	N/A	H-SIE-SIMA-180920/2983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PLC credentials. **CVE ID : CVE-2020-15791**		
simatic_s7-300_cpu_317f-2_dp					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	H-SIE-SIMA-180920/2984
simatic_s7-400_cpu_412					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	H-SIE-SIMA-180920/2985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
simatic_s7-400_cpu_414					
Insufficientl y Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	H-SIE-SIMA-180920/2986
simatic_s7-400_cpu_416					
Insufficientl y Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	H-SIE-SIMA-180920/2987
simatic_s7-400_cpu_417					
Insufficientl	09-Sep-20	3.3	A vulnerability has been	N/A	H-SIE-SIMA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
y Protected Credentials			identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**		180920/2988
simatic_hmi_comfort_panels					
Improper Restriction of Excessive Authentication Attempts	09-Sep-20	7.5	A vulnerability has been identified in SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions >= 14 and V < XX), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI Mobile Panels (All versions), SIMATIC HMI United Comfort Panels (All versions). Affected devices insufficiently block excessive authentication attempts. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack. **CVE ID : CVE-2020-15786**	N/A	H-SIE-SIMA-180920/2989
simatic_s7-300_cpu_314					
Insufficientl y Protected	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300	N/A	H-SIE-SIMA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**		180920/2990
simatic_s7-300_cpu_315-2_dp					
Insufficientl y Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	H-SIE-SIMA-180920/2991
simatic_hmi_basic_panels_2nd_generation					
Improper Restriction of Excessive Authenticat ion	09-Sep-20	7.5	A vulnerability has been identified in SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions >= 14 and V < XX),	N/A	H-SIE-SIMA-180920/2992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Attempts			SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI Mobile Panels (All versions), SIMATIC HMI United Comfort Panels (All versions). Affected devices insufficiently block excessive authentication attempts. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack. **CVE ID : CVE-2020-15786**		
simatic_hmi_mobile_panels					
Improper Restriction of Excessive Authentication Attempts	09-Sep-20	7.5	A vulnerability has been identified in SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions >= 14 and V < XX), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI Mobile Panels (All versions), SIMATIC HMI United Comfort Panels (All versions). Affected devices insufficiently block excessive authentication attempts. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack. **CVE ID : CVE-2020-15786**	N/A	H-SIE-SIMA-180920/2993
simatic_hmi_united_comfort_panels					
Improper Restriction of Excessive Authenticat	09-Sep-20	7.5	A vulnerability has been identified in SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All	N/A	H-SIE-SIMA-180920/2994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion Attempts			versions >= 14 and V < XX), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI Mobile Panels (All versions), SIMATIC HMI United Comfort Panels (All versions). Affected devices insufficiently block excessive authentication attempts. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack. **CVE ID : CVE-2020-15786**		
Improper Authentication	09-Sep-20	7.5	A vulnerability has been identified in SIMATIC HMI United Comfort Panels (All versions). Affected devices insufficiently validate authentication attempts as the information given can be truncated to match only a set number of characters versus the whole provided string. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack. **CVE ID : CVE-2020-15787**	N/A	H-SIE-SIMA-180920/2995
simatic_s7-300_cpu_312					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All	N/A	H-SIE-SIMA-180920/2996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**		
simatic_s7-300_cpu_315-2_pn					
Insufficientl y Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	H-SIE-SIMA-180920/2997
simatic_s7-300_cpu_317-2_pn					
Insufficientl y Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-	N/A	H-SIE-SIMA-180920/2998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**		
simatic_s7-300_cpu_317-2_dp					
Insufficiently Protected Credentials	09-Sep-20	3.3	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials. **CVE ID : CVE-2020-15791**	N/A	H-SIE-SIMA-180920/2999
Tendacn					
ac18					
Improper Authentication	04-Sep-20	6.8	Tenda AC18 Router through V15.03.05.05_EN and through V15.03.05.19(6318) CN devices could cause a remote code execution due to incorrect authentication handling of vulnerable logincheck() function in /usr/lib/lua/ngx_authserver/ngx_wdas.lua file if the administrator UI Interface is	N/A	H-TEN-AC18-180920/3000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			set to "radius". **CVE ID : CVE-2020-24987**		
ZTE					
zxr10_2800-4_almpufb\(low\)					
N/A	01-Sep-20	5	A ZTE product has a DoS vulnerability. Because the equipment couldn't distinguish the attack packets and normal packets with valid http links, the remote attackers could use this vulnerability to cause the equipment WEB/TELNET module denial of service and make the equipment be out of management. This affects: ZXR10 2800-4_ALMPUFB(LOW), all versions up to V3.00.40. **CVE ID : CVE-2020-6873**	N/A	H-ZTE-ZXR1-180920/3001
zxiptv					
Insufficientl y Protected Credentials	01-Sep-20	5.5	A ZTE product is impacted by the cryptographic issues vulnerability. The encryption algorithm is not properly used, so remote attackers could use this vulnerability for account credential enumeration attack or brute-force attack for password guessing. This affects: ZXIPTV, ZXIPTV-WEB-PV5.09.08.04. **CVE ID : CVE-2020-6874**	N/A	H-ZTE-ZXIP-180920/3002
Zyxel					
vmg5313-b30b					
Incorrect Permission	02-Sep-20	10	Zyxel VMG5313-B30B router on firmware	N/A	H-ZYX-VMG5-180920/3003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			5.13(ABCJ.6)b3_1127, and possibly older versions of firmware are affected by insecure permissions which allows regular and other users to create new users with elevated privileges. This is done by changing "FirstIndex" field in JSON that is POST-ed during account creation. Similar may also be possible with account deletion. **CVE ID : CVE-2020-24355**		