



National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Nov 2020

Vol. 07 No. 21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
absolunet					
kafe					
N/A	05-Nov-20	5	This affects the package @absolunet/kafe before 3.2.10. It allows cause a denial of service when validating crafted invalid emails. CVE ID : CVE-2020-7761	N/A	A-ABS-KAFE-181120/1
Adobe					
acrobat					
Out-of-bounds Read	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24426	N/A	A-ADO-ACRO-181120/2
Improper Input Validation	05-Nov-20	4.3	Acrobat Reader versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and	N/A	A-ADO-ACRO-181120/3

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
			earlier) are affected by an input validation vulnerability when decoding a crafted codec that could result in the disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24427		
Time-of-check Time-of-use (TOCTOU) Race Condition	05-Nov-20	5.1	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a time-of-check time-of-use (TOCTOU) race condition vulnerability that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24428	N/A	A-ADO-ACRO-181120/4
Improper Verification of Cryptographic Signature	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a signature verification bypass that could result in local privilege escalation. Exploitation of this issue requires user	N/A	A-ADO-ACRO-181120/5

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
			interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24429		
Use After Free	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability when handling malicious JavaScript. This vulnerability could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24430	N/A	A-ADO-ACRO-181120/6
Improper Authorization	05-Nov-20	5.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a security feature bypass that could result in dynamic library code injection by the Adobe Reader process. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24431	N/A	A-ADO-ACRO-181120/7
Improper Input Validation	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and	N/A	A-ADO-ACRO-181120/8

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
			earlier) and Adobe Acrobat Pro DC 2017.011.30175 (and earlier) are affected by an improper input validation vulnerability that could result in arbitrary JavaScript execution in the context of the current user. To exploit this issue, an attacker must acquire and then modify a certified PDF document that is trusted by the victim. The attacker then needs to convince the victim to open the document. CVE ID : CVE-2020-24432		
Improper Access Control	05-Nov-20	9.3	Adobe Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a local privilege escalation vulnerability that could enable a user without administrator privileges to delete arbitrary files and potentially execute arbitrary code as SYSTEM. Exploitation of this issue requires an attacker to socially engineer a victim, or the attacker must already have some access to the environment. CVE ID : CVE-2020-24433	N/A	A-ADO-ACRO-181120/9
Out-of-bounds Read	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and	N/A	A-ADO-ACRO-181120/10

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
			2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24434		
Heap-based Buffer Overflow	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a heap-based buffer overflow vulnerability in the submitForm function, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file in Acrobat Reader. CVE ID : CVE-2020-24435	N/A	A-ADO-ACRO-181120/11
Out-of-bounds Write	05-Nov-20	6.8	Acrobat Pro DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds write vulnerability that could result in writing past the end of an allocated memory	N/A	A-ADO-ACRO-181120/12

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
			structure. An attacker could leverage this vulnerability to execute code in the context of the current user. This vulnerability requires user interaction to exploit in that the victim must open a malicious document. CVE ID : CVE-2020-24436		
Use After Free	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24437	N/A	A-ADO-ACRO-181120/13
Use After Free	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability that could result in a memory address leak. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	A-ADO-ACRO-181120/14

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
			CVE ID : CVE-2020-24438		
acrobat_dc					
Out-of-bounds Read	05-Nov-20	4.3	<p>Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2020-24426</p>	N/A	A-ADO-ACRO-181120/15
Improper Input Validation	05-Nov-20	4.3	<p>Acrobat Reader versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an input validation vulnerability when decoding a crafted codec that could result in the disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2020-24427</p>	N/A	A-ADO-ACRO-181120/16
Time-of-	05-Nov-20	5.1	Acrobat Reader DC versions	N/A	A-ADO-ACRO-

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
check Time-of-use (TOCTOU) Race Condition			2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a time-of-check time-of-use (TOCTOU) race condition vulnerability that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24428		181120/17
Improper Verification of Cryptographic Signature	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a signature verification bypass that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24429	N/A	A-ADO-ACRO-181120/18
Use After Free	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability when handling malicious JavaScript. This vulnerability could result in arbitrary code execution in the context of the current user.	N/A	A-ADO-ACRO-181120/19

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
			Exploitation requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24430		
Improper Authorization	05-Nov-20	5.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a security feature bypass that could result in dynamic library code injection by the Adobe Reader process. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24431	N/A	A-ADO-ACRO-181120/20
Improper Input Validation	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) and Adobe Acrobat Pro DC 2017.011.30175 (and earlier) are affected by an improper input validation vulnerability that could result in arbitrary JavaScript execution in the context of the current user. To exploit this issue, an attacker must acquire and then modify a certified PDF document that is trusted by the victim. The attacker then needs to convince the victim to open the document.	N/A	A-ADO-ACRO-181120/21

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
			CVE ID : CVE-2020-24432		
Improper Access Control	05-Nov-20	9.3	<p>Adobe Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a local privilege escalation vulnerability that could enable a user without administrator privileges to delete arbitrary files and potentially execute arbitrary code as SYSTEM. Exploitation of this issue requires an attacker to socially engineer a victim, or the attacker must already have some access to the environment.</p> <p>CVE ID : CVE-2020-24433</p>	N/A	A-ADO-ACRO-181120/22
Out-of-bounds Read	05-Nov-20	4.3	<p>Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2020-24434</p>	N/A	A-ADO-ACRO-181120/23
Heap-based Buffer	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and	N/A	A-ADO-ACRO-

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
Overflow			earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a heap-based buffer overflow vulnerability in the submitForm function, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file in Acrobat Reader. CVE ID : CVE-2020-24435		181120/24
Out-of-bounds Write	05-Nov-20	6.8	Acrobat Pro DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds write vulnerability that could result in writing past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. This vulnerability requires user interaction to exploit in that the victim must open a malicious document. CVE ID : CVE-2020-24436	N/A	A-ADO-ACRO-181120/25
Use After Free	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a	N/A	A-ADO-ACRO-181120/26

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
			<p>use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user.</p> <p>Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2020-24437</p>		
Use After Free	05-Nov-20	4.3	<p>Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability that could result in a memory address leak.</p> <p>Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2020-24438</p>	N/A	A-ADO-ACRO-181120/27
acrobat_reader					
Out-of-bounds Read	05-Nov-20	4.3	<p>Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user</p>	N/A	A-ADO-ACRO-181120/28

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
			interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24426		
Improper Input Validation	05-Nov-20	4.3	Acrobat Reader versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an input validation vulnerability when decoding a crafted codec that could result in the disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24427	N/A	A-ADO-ACRO-181120/29
Time-of-check Time-of-use (TOCTOU) Race Condition	05-Nov-20	5.1	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a time-of-check time-of-use (TOCTOU) race condition vulnerability that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24428	N/A	A-ADO-ACRO-181120/30
Improper Verification	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and	N/A	A-ADO-ACRO-181120/31

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
of Cryptographic Signature			earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a signature verification bypass that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24429		
Use After Free	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability when handling malicious JavaScript. This vulnerability could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24430	N/A	A-ADO-ACRO-181120/32
Improper Authorization	05-Nov-20	5.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a security feature bypass that could result in dynamic library code injection by the Adobe Reader process. Exploitation of this issue requires user	N/A	A-ADO-ACRO-181120/33

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
			interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24431		
Improper Input Validation	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) and Adobe Acrobat Pro DC 2017.011.30175 (and earlier) are affected by an improper input validation vulnerability that could result in arbitrary JavaScript execution in the context of the current user. To exploit this issue, an attacker must acquire and then modify a certified PDF document that is trusted by the victim. The attacker then needs to convince the victim to open the document. CVE ID : CVE-2020-24432	N/A	A-ADO-ACRO-181120/34
Improper Access Control	05-Nov-20	9.3	Adobe Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a local privilege escalation vulnerability that could enable a user without administrator privileges to delete arbitrary files and potentially execute arbitrary code as SYSTEM. Exploitation of this issue requires an attacker to socially engineer a victim, or	N/A	A-ADO-ACRO-181120/35

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
			the attacker must already have some access to the environment. CVE ID : CVE-2020-24433		
Out-of-bounds Read	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24434	N/A	A-ADO-ACRO-181120/36
Heap-based Buffer Overflow	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a heap-based buffer overflow vulnerability in the submitForm function, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file in Acrobat Reader. CVE ID : CVE-2020-24435	N/A	A-ADO-ACRO-181120/37
Out-of-	05-Nov-20	6.8	Acrobat Pro DC versions	N/A	A-ADO-ACRO-

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
bounds Write			2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds write vulnerability that could result in writing past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. This vulnerability requires user interaction to exploit in that the victim must open a malicious document. CVE ID : CVE-2020-24436		181120/38
Use After Free	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24437	N/A	A-ADO-ACRO-181120/39
Use After Free	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and	N/A	A-ADO-ACRO-181120/40

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
			earlier) are affected by a use-after-free vulnerability that could result in a memory address leak. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24438		
acrobat_reader_dc					
Out-of-bounds Read	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24426	N/A	A-ADO-ACRO-181120/41
Improper Input Validation	05-Nov-20	4.3	Acrobat Reader versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an input validation vulnerability when decoding a crafted codec that could result in the disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass	N/A	A-ADO-ACRO-181120/42

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
			mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24427		
Time-of-check Time-of-use (TOCTOU) Race Condition	05-Nov-20	5.1	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a time-of-check time-of-use (TOCTOU) race condition vulnerability that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24428	N/A	A-ADO-ACRO-181120/43
Improper Verification of Cryptographic Signature	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a signature verification bypass that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24429	N/A	A-ADO-ACRO-181120/44
Use After Free	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and	N/A	A-ADO-ACRO-181120/45

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
			2017.011.30175 (and earlier) are affected by a use-after-free vulnerability when handling malicious JavaScript. This vulnerability could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24430		
Improper Authorization	05-Nov-20	5.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a security feature bypass that could result in dynamic library code injection by the Adobe Reader process. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24431	N/A	A-ADO-ACRO-181120/46
Improper Input Validation	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) and Adobe Acrobat Pro DC 2017.011.30175 (and earlier) are affected by an improper input validation vulnerability that could result in arbitrary JavaScript execution in the context of the current user. To exploit	N/A	A-ADO-ACRO-181120/47

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
			this issue, an attacker must acquire and then modify a certified PDF document that is trusted by the victim. The attacker then needs to convince the victim to open the document. CVE ID : CVE-2020-24432		
Improper Access Control	05-Nov-20	9.3	Adobe Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a local privilege escalation vulnerability that could enable a user without administrator privileges to delete arbitrary files and potentially execute arbitrary code as SYSTEM. Exploitation of this issue requires an attacker to socially engineer a victim, or the attacker must already have some access to the environment. CVE ID : CVE-2020-24433	N/A	A-ADO-ACRO-181120/48
Out-of-bounds Read	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as	N/A	A-ADO-ACRO-181120/49

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
			ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24434		
Heap-based Buffer Overflow	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a heap-based buffer overflow vulnerability in the submitForm function, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file in Acrobat Reader. CVE ID : CVE-2020-24435	N/A	A-ADO-ACRO-181120/50
Out-of-bounds Write	05-Nov-20	6.8	Acrobat Pro DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds write vulnerability that could result in writing past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. This vulnerability requires user interaction to exploit in that the victim must open a malicious document.	N/A	A-ADO-ACRO-181120/51

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
			CVE ID : CVE-2020-24436		
Use After Free	05-Nov-20	6.8	<p>Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2020-24437</p>	N/A	A-ADO-ACRO-181120/52
Use After Free	05-Nov-20	4.3	<p>Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability that could result in a memory address leak. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2020-24438</p>	N/A	A-ADO-ACRO-181120/53
Apache					
shiro					
Missing Authentication for Critical Function	05-Nov-20	7.5	Apache Shiro before 1.7.0, when using Apache Shiro with Spring, a specially crafted HTTP request may cause an authentication	N/A	A-APA-SHIR-181120/54

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
			bypass. CVE ID : CVE-2020-17510		
Arubanetworks					
airwave_glass					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-20	10	A remote unauthenticated arbitrary code execution vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2. CVE ID : CVE-2020-7128	N/A	A-ARU-AIRW-181120/55
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-20	9	A remote execution of arbitrary commands vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2. CVE ID : CVE-2020-7129	N/A	A-ARU-AIRW-181120/56
bbraun					
onlinesuite_application_package					
N/A	06-Nov-20	6.8	An Excel Macro Injection vulnerability exists in the export feature in the B. Braun OnlineSuite Version AP 3.0 and earlier via multiple input fields that are mishandled in an Excel export. CVE ID : CVE-2020-25170	N/A	A-BBR-ONLI-181120/57
Relative Path Traversal	06-Nov-20	7.5	A relative path traversal attack in the B. Braun OnlineSuite Version AP 3.0 and earlier allows unauthenticated attackers to upload or download arbitrary files.	N/A	A-BBR-ONLI-181120/58

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
			CVE ID : CVE-2020-25172		
Uncontrolled Search Path Element	06-Nov-20	6.9	A DLL hijacking vulnerability in the B. Braun OnlineSuite Version AP 3.0 and earlier allows local attackers to execute code on the system as a high privileged user. CVE ID : CVE-2020-25174	N/A	A-BBR-ONLI-181120/59
browserless					
chrome					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Nov-20	5	This affects all versions of package browserless-chrome. User input flowing from the workspace endpoint gets used to create a file path filePath and this is fetched and then sent back to a user. This can be escaped to fetch arbitrary files from a server. CVE ID : CVE-2020-7758	N/A	A-BRO-CHRO-181120/60
Cisco					
anyconnect_secure_mobility_client					
N/A	06-Nov-20	4.9	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to read arbitrary files on the underlying operating system of an affected device. The vulnerability is due to an exposed IPC function. An attacker could exploit this vulnerability by sending a crafted IPC message to the	N/A	A-CIS-ANYC-181120/61

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
			AnyConnect process on an affected device. A successful exploit could allow the attacker to read arbitrary files on the underlying operating system of the affected device. CVE ID : CVE-2020-27123		
Codection					
import_and_export_users_and_customers					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Nov-20	6	Import and export users and customers WordPress Plugin through 1.15.5.11 allows CSV injection via a customer's profile. CVE ID : CVE-2020-22277	N/A	A-COD-IMPO-181120/62
creativeitem					
neoflex_video_subscription_system					
Cross-Site Request Forgery (CSRF)	04-Nov-20	4.3	Neoflex Video Subscription System Version 2.0 is affected by CSRF which allows the Website's Settings to be changed (such as Payment Settings) CVE ID : CVE-2020-22273	N/A	A-CRE-NEOF-181120/63
databaseschemaviewer_project					
databaseschemaviewer					
Deserialization of Untrusted Data	04-Nov-20	6.8	DatabaseSchemaViewer before version 2.7.4.3 is vulnerable to arbitrary code execution if a user is tricked into opening a specially crafted `.dbschema` file. The patch was released in v2.7.4.3. As a workaround,	https://github.com/martinjw/dbschema-reader/security/advisories/GHSA-rfjh-	A-DAT-DATA-181120/64

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
			ensure `.dbschema` files from untrusted sources are not opened. CVE ID : CVE-2020-26207	m356-mpqf	
droppy_project					
droppy					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Nov-20	4	This affects all versions of package droppy. It is possible to traverse directories to fetch configuration files from a droopy server. CVE ID : CVE-2020-7757	N/A	A-DRO-DROP-181120/65
EA					
origin_client					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-20	3.5	A cross-site scripting (XSS) vulnerability exists in the Origin Client for Mac and PC 10.5.86 or earlier that could allow a remote attacker to execute arbitrary Javascript in a target user's Origin client. An attacker could use this vulnerability to access sensitive data related to the target user's Origin account, or to control or monitor the Origin text chat window. CVE ID : CVE-2020-15914	N/A	A-EA-ORIG-181120/66
easyregistrationforms					
easy_registration_forms					
Improper Neutralization of Special Elements in Output Used by a	04-Nov-20	6.8	Easy Registration Forms (ER Forms) Wordpress Plugin 2.0.6 allows an attacker to submit an entry with malicious CSV commands. After that, when the system	N/A	A-EAS-EASY-181120/67

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
Downstream Component ('Injection')			administrator generates CSV output from the forms information, there is no check on this inputs and the codes are executable. CVE ID : CVE-2020-22275		
evms					
redcap					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-20	3.5	A cross-site scripting (XSS) issue in REDCap 8.11.6 through 9.x before 10 allows attackers to inject arbitrary JavaScript or HTML in the Messenger feature. It was found that the filename of the image or file attached in a message could be used to perform this XSS attack. A user could craft a message and send it to anyone on the platform including admins. The XSS payload would execute on the other account without interaction from the user on several pages. CVE ID : CVE-2020-27359	N/A	A-EVM-REDC-181120/68
F5					
big-ip_ssl_orchestrator					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail	N/A	A-F5-BIG--181120/69

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
			and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939		
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943	N/A	A-F5-BIG--181120/70
big-ip_access_policy_manager					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939	N/A	A-F5-BIG--181120/71
Improper Neutralization of Input During Web	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability	N/A	A-F5-BIG--181120/72

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
Page Generation ('Cross-site Scripting')			exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940		
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943	N/A	A-F5-BIG--181120/73
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for resource admin to escalate to full admin. CVE ID : CVE-2020-5945	N/A	A-F5-BIG--181120/74
big-ip_advanced_firewall_manager					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC)	N/A	A-F5-BIG--181120/75

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
			card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940	N/A	A-F5-BIG--181120/76
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943	N/A	A-F5-BIG--181120/77
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for	N/A	A-F5-BIG--181120/78

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
			resource admin to escalate to full admin. CVE ID : CVE-2020-5945		
big-ip_analytics					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939	N/A	A-F5-BIG--181120/79
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940	N/A	A-F5-BIG--181120/80
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does.	N/A	A-F5-BIG--181120/81

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
			One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for resource admin to escalate to full admin. CVE ID : CVE-2020-5945	N/A	A-F5-BIG--181120/82
big-ip_application_acceleration_manager					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939	N/A	A-F5-BIG--181120/83
Improper Neutralization of Input During Web Page Generation ('Cross-site	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface	N/A	A-F5-BIG--181120/84

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
Scripting')			(TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940		
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943	N/A	A-F5-BIG--181120/85
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for resource admin to escalate to full admin. CVE ID : CVE-2020-5945	N/A	A-F5-BIG--181120/86
big-ip_application_security_manager					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail	N/A	A-F5-BIG--181120/87

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
			and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940	N/A	A-F5-BIG--181120/88
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943	N/A	A-F5-BIG--181120/89
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for resource admin to escalate to full admin. CVE ID : CVE-2020-5945	N/A	A-F5-BIG--181120/90

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
big-ip_domain_name_system					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939	N/A	A-F5-BIG--181120/91
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940	N/A	A-F5-BIG--181120/92
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password.	N/A	A-F5-BIG--181120/93

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
			CVE ID : CVE-2020-5943		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for resource admin to escalate to full admin. CVE ID : CVE-2020-5945	N/A	A-F5-BIG--181120/94
big-ip_edge_gateway					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940	N/A	A-F5-BIG--181120/95
big-ip_fraud_protection_service					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic.	N/A	A-F5-BIG--181120/96

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
			CVE ID : CVE-2020-5939		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940	N/A	A-F5-BIG--181120/97
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943	N/A	A-F5-BIG--181120/98
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for resource admin to escalate to full admin. CVE ID : CVE-2020-5945	N/A	A-F5-BIG--181120/99
big-ip_global_traffic_manager					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and	N/A	A-F5-BIG--181120/100

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
			13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940	N/A	A-F5-BIG--181120/101
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943	N/A	A-F5-BIG--181120/102
Improper Neutralization of Input	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed	N/A	A-F5-BIG--181120/103

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
During Web Page Generation ('Cross-site Scripting')			TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for resource admin to escalate to full admin. CVE ID : CVE-2020-5945		
big-ip_link_controller					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939	N/A	A-F5-BIG--181120/104
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940	N/A	A-F5-BIG--181120/105
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST	N/A	A-F5-BIG--181120/106

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
			interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for resource admin to escalate to full admin. CVE ID : CVE-2020-5945	N/A	A-F5-BIG--181120/107
big-ip_local_traffic_manager					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939	N/A	A-F5-BIG--181120/108
Improper Neutralization	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-	N/A	A-F5-BIG--181120/109

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
n of Input During Web Page Generation ('Cross-site Scripting')			14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940		
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943	N/A	A-F5-BIG--181120/110
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for resource admin to escalate to full admin. CVE ID : CVE-2020-5945	N/A	A-F5-BIG--181120/111
big-ip_policy_enforcement_manager					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-	N/A	A-F5-BIG--181120/112

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
			based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940	N/A	A-F5-BIG--181120/113
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943	N/A	A-F5-BIG--181120/114
Improper Neutralization of Input During Web Page Generation	05-Nov-20	8.5	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The	N/A	A-F5-BIG--181120/115

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
('Cross-site Scripting')			issue allows a minor privilege escalation for resource admin to escalate to full admin. CVE ID : CVE-2020-5945		
big-ip_webaccelerator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. CVE ID : CVE-2020-5940	N/A	A-F5-BIG--181120/116
big-ip_advanced_web_application_firewall					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939	N/A	A-F5-BIG--181120/117
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the	N/A	A-F5-BIG--181120/118

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
			REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943		
big-ip_ddos_hybrid_defender					
N/A	05-Nov-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic. CVE ID : CVE-2020-5939	N/A	A-F5-BIG--181120/119
Inadequate Encryption Strength	05-Nov-20	4	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password. CVE ID : CVE-2020-5943	N/A	A-F5-BIG--181120/120
Foxitsoftware					

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
foxit_reader					
N/A	02-Nov-20	6.8	Foxit Reader before 10.0 allows Remote Command Execution via the app.openPDFWebPage JavaScript API. An attacker can execute local files and bypass the security dialog. CVE ID : CVE-2020-14425	N/A	A-FOX-FOXI-181120/121
fruitywifi_project					
fruitywifi					
Improper Encoding or Escaping of Output	05-Nov-20	6.5	A remote code execution vulnerability is identified in FruityWifi through 2.4. Due to improperly escaped shell metacharacters obtained from the POST request at the page_config_adv.php page, it is possible to perform remote code execution by an authenticated attacker. This is similar to CVE-2018-17317. CVE ID : CVE-2020-24849	N/A	A-FRU-FRUI-181120/122
git_large_file_storage_project					
git_large_file_storage					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Nov-20	10	Git LFS 2.12.0 allows Remote Code Execution. CVE ID : CVE-2020-27955	N/A	A-GIT-GIT_-181120/123
Google					
chrome					
Use After	03-Nov-20	6.8	Use after free in payments in	N/A	A-GOO-CHRO-

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
Free			Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15967		181120/124
Use After Free	03-Nov-20	6.8	Use after free in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15968	N/A	A-GOO-CHRO-181120/125
Use After Free	03-Nov-20	6.8	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15969	N/A	A-GOO-CHRO-181120/126
Use After Free	03-Nov-20	6.8	Use after free in NFC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15970	N/A	A-GOO-CHRO-181120/127
Use After Free	03-Nov-20	6.8	Use after free in printing in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape	N/A	A-GOO-CHRO-181120/128

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
			via a crafted HTML page. CVE ID : CVE-2020-15971		
Use After Free	03-Nov-20	6.8	Use after free in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15972	N/A	A-GOO-CHRO-181120/129
N/A	03-Nov-20	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 86.0.4240.75 allowed an attacker who convinced a user to install a malicious extension to bypass same origin policy via a crafted Chrome Extension. CVE ID : CVE-2020-15973	N/A	A-GOO-CHRO-181120/130
Integer Overflow or Wraparound	03-Nov-20	6.8	Integer overflow in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to bypass site isolation via a crafted HTML page. CVE ID : CVE-2020-15974	N/A	A-GOO-CHRO-181120/131
Integer Overflow or Wraparound	03-Nov-20	6.8	Integer overflow in SwiftShader in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15975	N/A	A-GOO-CHRO-181120/132
Use After Free	03-Nov-20	6.8	Use after free in WebXR in Google Chrome on Android	N/A	A-GOO-CHRO-181120/133

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
			prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15976		
Improper Input Validation	03-Nov-20	4.3	Insufficient data validation in dialogs in Google Chrome on OS X prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page. CVE ID : CVE-2020-15977	N/A	A-GOO-CHRO-181120/134
Improper Input Validation	03-Nov-20	6.8	Insufficient data validation in navigation in Google Chrome on Android prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. CVE ID : CVE-2020-15978	N/A	A-GOO-CHRO-181120/135
N/A	03-Nov-20	6.8	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15979	N/A	A-GOO-CHRO-181120/136
N/A	03-Nov-20	4.6	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 86.0.4240.75 allowed a local attacker to	N/A	A-GOO-CHRO-181120/137

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
			bypass navigation restrictions via crafted Intents. CVE ID : CVE-2020-15980		
Out-of-bounds Read	03-Nov-20	4.3	Out of bounds read in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. CVE ID : CVE-2020-15981	N/A	A-GOO-CHRO-181120/138
N/A	03-Nov-20	4.3	Inappropriate implementation in cache in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. CVE ID : CVE-2020-15982	N/A	A-GOO-CHRO-181120/139
Improper Input Validation	03-Nov-20	4.4	Insufficient data validation in webUI in Google Chrome on ChromeOS prior to 86.0.4240.75 allowed a local attacker to bypass content security policy via a crafted HTML page. CVE ID : CVE-2020-15983	N/A	A-GOO-CHRO-181120/140
N/A	03-Nov-20	4.3	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 86.0.4240.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted URL.	N/A	A-GOO-CHRO-181120/141

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
			CVE ID : CVE-2020-15984		
N/A	03-Nov-20	4.3	Inappropriate implementation in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to spoof security UI via a crafted HTML page. CVE ID : CVE-2020-15985	N/A	A-GOO-CHRO-181120/142
Use After Free	03-Nov-20	4.3	Integer overflow in media in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15986	N/A	A-GOO-CHRO-181120/143
Use After Free	03-Nov-20	6.8	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted WebRTC stream. CVE ID : CVE-2020-15987	N/A	A-GOO-CHRO-181120/144
N/A	03-Nov-20	6.8	Insufficient policy enforcement in downloads in Google Chrome on Windows prior to 86.0.4240.75 allowed a remote attacker who convinced the user to open files to execute arbitrary code via a crafted HTML page. CVE ID : CVE-2020-15988	N/A	A-GOO-CHRO-181120/145
Improper Initialization	03-Nov-20	4.3	Uninitialized data in PDFium in Google Chrome prior to	N/A	A-GOO-CHRO-181120/146

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
			86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file. CVE ID : CVE-2020-15989		
Use After Free	03-Nov-20	6.8	Use after free in autofill in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15990	N/A	A-GOO-CHRO-181120/147
Use After Free	03-Nov-20	6.8	Use after free in password manager in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15991	N/A	A-GOO-CHRO-181120/148
N/A	03-Nov-20	6.8	Insufficient policy enforcement in networking in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. CVE ID : CVE-2020-15992	N/A	A-GOO-CHRO-181120/149
Use After Free	03-Nov-20	6.8	Use after free in printing in Google Chrome prior to 86.0.4240.99 allowed a	N/A	A-GOO-CHRO-181120/150

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
			remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15993		
Use After Free	03-Nov-20	6.8	Use after free in V8 in Google Chrome prior to 86.0.4240.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15994	N/A	A-GOO-CHRO-181120/151
Out-of-bounds Write	03-Nov-20	6.8	Out of bounds write in V8 in Google Chrome prior to 86.0.4240.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15995	N/A	A-GOO-CHRO-181120/152
Use After Free	03-Nov-20	6.8	Use after free in passwords in Google Chrome prior to 86.0.4240.99 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15996	N/A	A-GOO-CHRO-181120/153
Use After Free	03-Nov-20	6.8	Use after free in Mojo in Google Chrome prior to 86.0.4240.99 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	N/A	A-GOO-CHRO-181120/154

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
			CVE ID : CVE-2020-15997		
Use After Free	03-Nov-20	6.8	Use after free in USB in Google Chrome prior to 86.0.4240.99 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15998	N/A	A-GOO-CHRO-181120/155
Out-of-bounds Write	03-Nov-20	4.3	Heap buffer overflow in Freetype in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15999	N/A	A-GOO-CHRO-181120/156
Out-of-bounds Write	03-Nov-20	6.8	Inappropriate implementation in Blink in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16000	N/A	A-GOO-CHRO-181120/157
Use After Free	03-Nov-20	6.8	Use after free in media in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16001	N/A	A-GOO-CHRO-181120/158
Use After Free	03-Nov-20	6.8	Use after free in PDFium in Google Chrome prior to 86.0.4240.111 allowed a	N/A	A-GOO-CHRO-181120/159

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
			remote attacker to potentially exploit heap corruption via a crafted PDF file. CVE ID : CVE-2020-16002		
Use After Free	03-Nov-20	6.8	Use after free in printing in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16003	N/A	A-GOO-CHRO-181120/160
Use After Free	03-Nov-20	6.8	Use after free in user interface in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16004	N/A	A-GOO-CHRO-181120/161
Out-of-bounds Write	03-Nov-20	6.8	Insufficient policy enforcement in ANGLE in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16005	N/A	A-GOO-CHRO-181120/162
Out-of-bounds Write	03-Nov-20	6.8	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	N/A	A-GOO-CHRO-181120/163

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
			CVE ID : CVE-2020-16006		
Improper Input Validation	03-Nov-20	4.6	Insufficient data validation in installer in Google Chrome prior to 86.0.4240.183 allowed a local attacker to potentially elevate privilege via a crafted filesystem. CVE ID : CVE-2020-16007	N/A	A-GOO-CHRO-181120/164
Out-of-bounds Write	03-Nov-20	7.5	Stack buffer overflow in WebRTC in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit stack corruption via a crafted WebRTC packet. CVE ID : CVE-2020-16008	N/A	A-GOO-CHRO-181120/165
Out-of-bounds Write	03-Nov-20	6.8	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16009	N/A	A-GOO-CHRO-181120/166
Out-of-bounds Write	03-Nov-20	6.8	Heap buffer overflow in UI in Google Chrome on Android prior to 86.0.4240.185 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-16010	N/A	A-GOO-CHRO-181120/167
Out-of-bounds Write	03-Nov-20	7.5	Heap buffer overflow in UI in Google Chrome on Windows prior to 86.0.4240.183	N/A	A-GOO-CHRO-181120/168

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
			allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-16011		
N/A	03-Nov-20	4.3	Inappropriate implementation in networking in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page. CVE ID : CVE-2020-6557	N/A	A-GOO-CHRO-181120/169
hashicorp					
consul					
Excessive Iteration	04-Nov-20	5	HashiCorp Consul Enterprise version 1.7.0 up to 1.8.4 includes a namespace replication bug which can be triggered to cause denial of service via infinite Raft writes. Fixed in 1.7.9 and 1.8.5. CVE ID : CVE-2020-25201	https://github.com/hashicorp/consul/blob/master/CHANGELOG.md#185-october-23-2020	A-HAS-CONS-181120/170
hcltech					
hcl_digital_experience					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	4.3	HCL Digital Experience 8.5, 9.0, 9.5 is susceptible to cross site scripting (XSS). One subcomponent is vulnerable to reflected XSS. In reflected XSS, an attacker must induce a victim to click on a crafted URL from some	N/A	A-HCL-HCL_-181120/171

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
			delivery mechanism (email, other web site). CVE ID : CVE-2020-14222		
horizontcms_project					
horizontcms					
Unrestricted Upload of File with Dangerous Type	05-Nov-20	6.5	An unrestricted file upload issue in HorizontCMS through 1.0.0-beta allows an authenticated remote attacker (with access to the FileManager) to upload and execute arbitrary PHP code by uploading a PHP payload, and then using the FileManager's rename function to provide the payload (which will receive a random name on the server) with the PHP extension, and finally executing the PHP file via an HTTP GET request to /storage/<php_file_name>. NOTE: the vendor has patched this while leaving the version number at 1.0.0-beta. CVE ID : CVE-2020-27387	N/A	A-HOR-HORI-181120/172
HP					
synergy_composer					
Improper Privilege Management	06-Nov-20	6.5	There is a remote escalation of privilege possible for a malicious user that has a OneView account in OneView and Synergy Composer. HPE has provided updates to Oneview and Synergy Composer: Update to version 5.5 of OneView,	N/A	A-HP-SYNE-181120/173

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
			Composer, or Composer2. CVE ID : CVE-2020-7198		
synergy_composer_2					
Improper Privilege Management	06-Nov-20	6.5	There is a remote escalation of privilege possible for a malicious user that has a OneView account in OneView and Synergy Composer. HPE has provided updates to Oneview and Synergy Composer: Update to version 5.5 of OneView, Composer, or Composer2. CVE ID : CVE-2020-7198	N/A	A-HP-SYNE-181120/174
oneview					
Improper Privilege Management	06-Nov-20	6.5	There is a remote escalation of privilege possible for a malicious user that has a OneView account in OneView and Synergy Composer. HPE has provided updates to Oneview and Synergy Composer: Update to version 5.5 of OneView, Composer, or Composer2. CVE ID : CVE-2020-7198	N/A	A-HP-ONEV-181120/175
IBM					
urbancode_deploy					
Incorrect Authorization	06-Nov-20	4	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 7.0.3.0, and 7.0.4.0 could allow an authenticated user to bypass security. A user with access to a snapshot could apply unauthorized additional statuses via direct rest calls. IBM X-Force ID: 181856.	https://www.ibm.com/support/pages/node/6337603	A-IBM-URBA-181120/176

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
			CVE ID : CVE-2020-4482		
Information Exposure Through an Error Message	06-Nov-20	4	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 7.0.3.0, and 7.0.4.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 181857. CVE ID : CVE-2020-4483	https://www.ibm.com/support/pages/node/6360835	A-IBM-URBA-181120/177
Information Exposure	06-Nov-20	4	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 7.0.3.0, and 7.0.4.0 could disclose sensitive information to an authenticated user that could be used in further attacks against the system. IBM X-Force ID: 181858. CVE ID : CVE-2020-4484	https://www.ibm.com/support/pages/node/6337605	A-IBM-URBA-181120/178
planning_analytics_local					
Information Exposure	03-Nov-20	4	IBM Planning Analytics Local 2.0.9.2 and IBM Planning Analytics Workspace 57 could expose data to non-privileged users by not invalidating TM1Web user sessions. IBM X-Force ID: 186022. CVE ID : CVE-2020-4649	https://www.ibm.com/support/pages/node/6356539	A-IBM-PLAN-181120/179
filenet_content_manager					
N/A	09-Nov-20	9.3	IBM FileNet Content Manager 5.5.4 and 5.5.5 is potentially vulnerable to CVS Injection. A remote attacker could execute arbitrary	https://www.ibm.com/support/pages/node/6336	A-IBM-FILE-181120/180

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
			commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 188736. CVE ID : CVE-2020-4759	917	
maximo_spatial_asset_management					
Information Exposure	09-Nov-20	2.1	IBM Maximo Spatial Asset Management 7.6.0.3, 7.6.0.4, 7.6.0.5, and 7.6.1.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 186023. CVE ID : CVE-2020-4650	https://www.ibm.com/support/pages/node/6361769	A-IBM-MAXI-181120/181
Cross-Site Request Forgery (CSRF)	09-Nov-20	2.9	IBM Maximo Spatial Asset Management 7.6.0.3, 7.6.0.4, 7.6.0.5, and 7.6.1.0 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: 186024. CVE ID : CVE-2020-4651	https://www.ibm.com/support/pages/node/6361767	A-IBM-MAXI-181120/182
app_connect_enterprise_certified_container					
Improper Restriction of Rendered UI Layers or Frames	03-Nov-20	4.9	IBM App Connect Enterprise Certified Container 1.0.0, 1.0.1, 1.0.2, 1.0.3, and 1.0.4 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch	https://www.ibm.com/support/pages/node/6357899	A-IBM-APP_-181120/183

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
			further attacks against the victim. IBM X-Force ID: 189219. CVE ID : CVE-2020-4785		
Icewarp					
mail_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-20	4.3	IceWarp 11.4.5.0 allows XSS via the language parameter. CVE ID : CVE-2020-27982	N/A	A-ICE-MAIL-181120/184
immuta					
immuta					
Weak Password Recovery Mechanism for Forgotten Password	05-Nov-20	5	Immuta v2.8.2 is affected by one instance of insecure permissions that can lead to user account takeover. CVE ID : CVE-2020-15949	N/A	A-IMM-IMMU-181120/185
Insufficient Session Expiration	05-Nov-20	6.8	Immuta v2.8.2 is affected by improper session management: user sessions are not revoked upon logout. CVE ID : CVE-2020-15950	N/A	A-IMM-IMMU-181120/186
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Nov-20	4.3	Immuta v2.8.2 accepts user-supplied project names without properly sanitizing the input, allowing attackers to inject arbitrary HTML content that is rendered as part of the application. An attacker could leverage this to redirect application users to a phishing website in an attempt to steal credentials.	N/A	A-IMM-IMMU-181120/187

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
			CVE ID : CVE-2020-15951		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	6	<p>Immuta v2.8.2 is affected by stored XSS that allows a low-privileged user to escalate privileges to administrative permissions. Additionally, unauthenticated attackers can phish unauthenticated Immuta users to steal credentials or force actions on authenticated users through reflected, DOM-based XSS.</p> <p>CVE ID : CVE-2020-15952</p>	N/A	A-IMM-IMMU-181120/188
Jenkins					
vmware_lab_manager_slaves					
Unprotected Storage of Credentials	04-Nov-20	4	<p>Jenkins VMware Lab Manager Slaves Plugin 0.2.8 and earlier stores a password unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.</p> <p>CVE ID : CVE-2020-2319</p>	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2084	A-JEN-VMWA-181120/189
mercurial					
Improper Restriction of XML External Entity Reference ('XXE')	04-Nov-20	4	<p>Jenkins Mercurial Plugin 2.11 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.</p> <p>CVE ID : CVE-2020-2305</p>	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2115	A-JEN-MERC-181120/190
Missing Authorization	04-Nov-20	4	<p>A missing permission check in Jenkins Mercurial Plugin 2.11 and earlier allows</p>	https://www.jenkins.io/security/	A-JEN-MERC-181120/191

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
			attackers with Overall/Read permission to obtain a list of names of configured Mercurial installations. CVE ID : CVE-2020-2306	ty/advisory/2020-11-04/#SECURITY-2104	
kubernetes					
Information Exposure	04-Nov-20	4	Jenkins Kubernetes Plugin 1.27.3 and earlier allows low-privilege users to access possibly sensitive Jenkins controller environment variables. CVE ID : CVE-2020-2307	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-1646	A-JEN-KUBE-181120/192
Missing Authorization	04-Nov-20	4	A missing permission check in Jenkins Kubernetes Plugin 1.27.3 and earlier allows attackers with Overall/Read permission to list global pod template names. CVE ID : CVE-2020-2308	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2102	A-JEN-KUBE-181120/193
Missing Authorization	04-Nov-20	4	A missing/An incorrect permission check in Jenkins Kubernetes Plugin 1.27.3 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. CVE ID : CVE-2020-2309	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2103	A-JEN-KUBE-181120/194
ansible					
Missing Authorization	04-Nov-20	4	Missing permission checks in Jenkins Ansible Plugin 1.0 and earlier allow attackers with Overall/Read permission to enumerate credentials IDs of credentials	https://www.jenkins.io/security/advisory/2020-11-04/#SECU	A-JEN-ANSI-181120/195

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
			stored in Jenkins. CVE ID : CVE-2020-2310	RITY-1943	
aws_global_configuration					
Missing Authorization	04-Nov-20	4	A missing permission check in Jenkins AWS Global Configuration Plugin 1.5 and earlier allows attackers with Overall/Read permission to replace the global AWS configuration. CVE ID : CVE-2020-2311	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2101	A-JEN-AWS-181120/196
sqlplus_script_runner					
Insufficiently Protected Credentials	04-Nov-20	4	Jenkins SQLPlus Script Runner Plugin 2.0.12 and earlier does not mask a password provided as command line argument in build logs. CVE ID : CVE-2020-2312	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2129	A-JEN-SQLP-181120/197
azure_key_vault					
Missing Authorization	04-Nov-20	4	A missing permission check in Jenkins Azure Key Vault Plugin 2.0 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. CVE ID : CVE-2020-2313	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2110	A-JEN-AZUR-181120/198
appspider					
Unprotected Storage of Credentials	04-Nov-20	2.1	Jenkins AppSpider Plugin 1.0.12 and earlier stores a password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2110	A-JEN-APPS-181120/199

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
			controller file system. CVE ID : CVE-2020-2314	RITY-2058	
visualworks_store					
Improper Restriction of XML External Entity Reference ('XXE')	04-Nov-20	4	Jenkins Visualworks Store Plugin 1.1.3 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. CVE ID : CVE-2020-2315	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-1900	A-JEN-VISU-181120/200
findbugs					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-20	3.5	Jenkins FindBugs Plugin 5.0.0 and earlier does not escape the annotation message in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide report files to Jenkins FindBugs Plugin's post build step. CVE ID : CVE-2020-2317	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-1918	A-JEN-FIND-181120/201
mail_commander					
Unprotected Storage of Credentials	04-Nov-20	4	Jenkins Mail Commander Plugin for Jenkins-ci Plugin 1.0.0 and earlier stores passwords unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission, or access to the Jenkins controller file system. CVE ID : CVE-2020-2318	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2085	A-JEN-MAIL-181120/202
active_directory					

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
Improper Authentication	04-Nov-20	7.5	Jenkins Active Directory Plugin 2.19 and earlier allows attackers to log in as any user if a magic constant is used as the password. CVE ID : CVE-2020-2299	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2117	A-JEN-ACTI-181120/203
Improper Authentication	04-Nov-20	7.5	Jenkins Active Directory Plugin 2.19 and earlier does not prohibit the use of an empty password in Windows/ADSI mode, which allows attackers to log in to Jenkins as any user depending on the configuration of the Active Directory server. CVE ID : CVE-2020-2300	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2099	A-JEN-ACTI-181120/204
Improper Authentication	04-Nov-20	7.5	Jenkins Active Directory Plugin 2.19 and earlier allows attackers to log in as any user with any password while a successful authentication of that user is still in the optional cache when using Windows/ADSI mode. CVE ID : CVE-2020-2301	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2123	A-JEN-ACTI-181120/205
Missing Authorization	04-Nov-20	4	A missing permission check in Jenkins Active Directory Plugin 2.19 and earlier allows attackers with Overall/Read permission to access the domain health check diagnostic page. CVE ID : CVE-2020-2302	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-1999	A-JEN-ACTI-181120/206
Cross-Site Request	04-Nov-20	4.3	A cross-site request forgery (CSRF) vulnerability in	https://www.jenkins.io	A-JEN-ACTI-181120/207

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
Forgery (CSRF)			Jenkins Active Directory Plugin 2.19 and earlier allows attackers to perform connection tests, connecting to attacker-specified or previously configured Active Directory servers using attacker-specified credentials. CVE ID : CVE-2020-2303	s.io/security/advisory/2020-11-04/#SECURITY-2126	
subversion					
Improper Restriction of XML External Entity Reference ('XXE')	04-Nov-20	4	Jenkins Subversion Plugin 2.13.1 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. CVE ID : CVE-2020-2304	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2145	A-JEN-SUBV-181120/208
static_analysis_utilities					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-20	3.5	Jenkins Static Analysis Utilities Plugin 1.96 and earlier does not escape the annotation message in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission. CVE ID : CVE-2020-2316	https://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-1907	A-JEN-STAT-181120/209
jomsocial					
jomsocial					
N/A	04-Nov-20	7.5	JomSocial (Joomla Social Network Extention) 4.7.6 allows CSV injection via a customer's profile. CVE ID : CVE-2020-22274	N/A	A-JOM-JOMS-181120/210

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
joplin_project					
joplin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Nov-20	4.3	Joplin 1.2.6 for Desktop allows XSS via a LINK element in a note. CVE ID : CVE-2020-28249	N/A	A-JOP-JOPL-181120/211
jsreport					
jsreport-chrome-pdf					
Information Exposure	05-Nov-20	4	This affects the package jsreport-chrome-pdf before 1.10.0. CVE ID : CVE-2020-7762	N/A	A-JSR-JSRE-181120/212
phantom-html-to-pdf					
Information Exposure	05-Nov-20	5	This affects the package phantom-html-to-pdf before 0.6.1. CVE ID : CVE-2020-7763	N/A	A-JSR-PHAN-181120/213
lightbend					
play_framework					
Uncontrolled Recursion	06-Nov-20	5	In Play Framework 2.6.0 through 2.8.2, data amplification can occur when an application accepts multipart/form-data JSON input. CVE ID : CVE-2020-26882	N/A	A-LIG-PLAY-181120/214
Uncontrolled Recursion	06-Nov-20	5	In Play Framework 2.6.0 through 2.8.2, stack consumption can occur because of unbounded recursion during parsing of crafted JSON documents.	N/A	A-LIG-PLAY-181120/215

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
			CVE ID : CVE-2020-26883		
Out-of-bounds Write	06-Nov-20	5	An issue was discovered in PlayJava in Play Framework 2.6.0 through 2.8.2. The body parsing of HTTP requests eagerly parses a payload given a Content-Type header. A deep JSON structure sent to a valid POST endpoint (that may or may not expect JSON payloads) causes a StackOverflowError and Denial of Service. CVE ID : CVE-2020-27196	N/A	A-LIG-PLAY-181120/216
Linuxfoundation					
nats-server					
NULL Pointer Dereference	06-Nov-20	5	The JWT library in NATS nats-server before 2.1.9 allows a denial of service (a nil dereference in Go code). CVE ID : CVE-2020-26521	http://www.openwall.com/lists/oss-security/2020/11/02/2	A-LIN-NATS-181120/217
Use of Hard-coded Credentials	06-Nov-20	7.5	The JWT library in NATS nats-server before 2.1.9 has Incorrect Access Control because of how expired credentials are handled. CVE ID : CVE-2020-26892	https://www.openwall.com/lists/oss-security/2020/11/02/2	A-LIN-NATS-181120/218
Magento					
magento					
Improper Neutralization of Special Elements used in an	09-Nov-20	5.5	Magento versions 2.4.0 and 2.3.5 (and earlier) are affected by an SQL Injection vulnerability that could lead to sensitive information	N/A	A-MAG-MAGE-181120/219

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
SQL Command ('SQL Injection')			disclosure. This vulnerability could be exploited by an authenticated user with permissions to the product listing page to read data from the database. CVE ID : CVE-2020-24400		
Incorrect Authorization	09-Nov-20	5.5	Magento versions 2.4.0 and 2.3.5p1 (and earlier) are affected by an incorrect authorization vulnerability. A user can still access resources provisioned under their old role after an administrator removes the role or disables the user's account. CVE ID : CVE-2020-24401	N/A	A-MAG-MAGE-181120/220
Improper Authorization	09-Nov-20	5.5	Magento version 2.4.0 and 2.3.5p1 (and earlier) are affected by an incorrect permissions vulnerability in the Integrations component. This vulnerability could be abused by authenticated users with permissions to the Resource Access API to delete customer details via the REST API without authorization. CVE ID : CVE-2020-24402	N/A	A-MAG-MAGE-181120/221
Improper Authorization	09-Nov-20	4	Magento version 2.4.0 and 2.3.5p1 (and earlier) are affected by an incorrect user permissions vulnerability within the Inventory component. This vulnerability could be abused by authenticated	N/A	A-MAG-MAGE-181120/222

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
			users with Inventory and Source permissions to make unauthorized changes to inventory source data via the REST API. CVE ID : CVE-2020-24403		
Improper Authorization	09-Nov-20	5.5	Magento version 2.4.0 and 2.3.5p1 (and earlier) are affected by an incorrect permissions vulnerability within the Integrations component. This vulnerability could be abused by users with permissions to the Pages resource to delete cms pages via the REST API without authorization. CVE ID : CVE-2020-24404	N/A	A-MAG-MAGE-181120/223
Improper Authorization	09-Nov-20	4	Magento version 2.4.0 and 2.3.5p1 (and earlier) are affected by an incorrect permissions issue vulnerability in the Inventory module. This vulnerability could be abused by authenticated users to modify inventory stock data without authorization. CVE ID : CVE-2020-24405	N/A	A-MAG-MAGE-181120/224
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Nov-20	4.3	When in maintenance mode, Magento version 2.4.0 and 2.3.4 (and earlier) are affected by an information disclosure vulnerability that could expose the installation path during build deployments. This	N/A	A-MAG-MAGE-181120/225

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
			information could be helpful to attackers if they are able to identify other exploitable vulnerabilities in the environment. CVE ID : CVE-2020-24406		
Unrestricted Upload of File with Dangerous Type	09-Nov-20	9	Magento versions 2.4.0 and 2.3.5p1 (and earlier) are affected by an unsafe file upload vulnerability that could result in arbitrary code execution. This vulnerability could be abused by authenticated users with administrative permissions to the System/Data and Transfer/Import components. CVE ID : CVE-2020-24407	N/A	A-MAG-MAGE-181120/226
marmind					
marmind					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	4.3	A Stored Cross-Site Scripting (XSS) vulnerability in the "Marmind" web application with version 4.1.141.0 allows an attacker to inject code that will later be executed by legitimate users when they open the assets containing the JavaScript code. This would allow an attacker to perform unauthorized actions in the application on behalf of legitimate users or spread malware via the application. By using the "Assets Upload" function, an attacker can	N/A	A-MAR-MARM-181120/227

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
			abuse the upload function to upload a malicious PDF file containing a stored XSS. CVE ID : CVE-2020-26505		
mind					
imind_server					
N/A	05-Nov-20	6.8	CSV Injection exists in InterMind iMind Server through 3.13.65 via the csv export functionality. CVE ID : CVE-2020-25398	N/A	A-MIN-IMIN-181120/228
Insufficiently Protected Credentials	05-Nov-20	6.8	Stored XSS in InterMind iMind Server through 3.13.65 allows any user to hijack another user's session by sending a malicious file in the chat. CVE ID : CVE-2020-25399	N/A	A-MIN-IMIN-181120/229
Moxa					
mxview					
Improper Privilege Management	05-Nov-20	7.2	An exploitable local privilege elevation vulnerability exists in the file system permissions of Moxa MXView series 3.1.8 installation. Depending on the vector chosen, an attacker can either add code to a script or replace a binary. By default MXViewService, which starts as a NT SYSTEM authority user executes a series of Node.js scripts to start additional application functionality. CVE ID : CVE-2020-13536	N/A	A-MOX-MXVI-181120/230

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
Improper Privilege Management	05-Nov-20	7.2	An exploitable local privilege elevation vulnerability exists in the file system permissions of Moxa MXView series 3.1.8 installation. Depending on the vector chosen, an attacker can either add code to a script or replace a binary. By default MXViewService, which starts as a NT SYSTEM authority user executes a series of Node.js scripts to start additional application functionality and among them the mosquito executable is also run. CVE ID : CVE-2020-13537	N/A	A-MOX-MXVI-181120/231
nedi					
nedi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-20	3.5	NeDi 1.9C allows inc/rt-popup.php d XSS. CVE ID : CVE-2020-23868	N/A	A-NED-NEDI-181120/232
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-20	3.5	NeDi 1.9C allows pwsec.php oid XSS. CVE ID : CVE-2020-23989	N/A	A-NED-NEDI-181120/233
Netapp					
e-series_santricity_os_controller					

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
N/A	06-Nov-20	4.3	SANtricity OS Controller Software versions 11.50.1 and higher are susceptible to a vulnerability which could allow an attacker to discover sensitive information by intercepting its transmission within an https session. CVE ID : CVE-2020-8577	N/A	A-NET-E-SE-181120/234
N/A	06-Nov-20	5	SANtricity OS Controller Software versions 11.30 and higher are susceptible to a vulnerability which allows an unauthenticated attacker with access to the system to cause a Denial of Service (DoS). CVE ID : CVE-2020-8580	N/A	A-NET-E-SE-181120/235
Netiq					
self_service_password_reset					
Information Exposure	05-Nov-20	5	Sensitive information disclosure vulnerability in Micro Focus Self Service Password Reset (SSPR) product. The vulnerability affects versions 4.4.0.0 to 4.4.0.6 and 4.5.0.1 and 4.5.0.2. In certain configurations the vulnerability could disclose sensitive information. CVE ID : CVE-2020-25837	N/A	A-NET-SELF-181120/236
Nextcloud					
nextcloud					
Insufficiently Protected Credentials	02-Nov-20	5	A logic error in Nextcloud Server 19.0.0 caused a plaintext storage of the share password when it was	N/A	A-NEX-NEXT-181120/237

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
			given on the initial create API call. CVE ID : CVE-2020-8183		
oleacorn					
olea_gift_on_order					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Nov-20	5	The Module Olea Gift On Order module through 5.0.8 for PrestaShop enables an unauthenticated user to read arbitrary files on the server via <code>getfile.php?file=../</code> directory traversal. CVE ID : CVE-2020-9368	N/A	A-OLE-OLEA-181120/238
openfind					
mailaudit					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Nov-20	9	MailGates and MailAudit products contain Command Injection flaw, which can be used to inject and execute system commands from the cgi parameter after attackers obtain the user's access token. CVE ID : CVE-2020-25849	https://www.twcert.org.tw/tw/cp-132-4118-6292c-1.html	A-OPE-MAIL-181120/239
mailgates					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Nov-20	9	MailGates and MailAudit products contain Command Injection flaw, which can be used to inject and execute system commands from the cgi parameter after attackers obtain the user's access token. CVE ID : CVE-2020-25849	https://www.twcert.org.tw/tw/cp-132-4118-6292c-1.html	A-OPE-MAIL-181120/240
Opensuse					
backports_sle					

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
Use After Free	03-Nov-20	6.8	Use after free in payments in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15967	N/A	A-OPE-BACK-181120/241
Use After Free	03-Nov-20	6.8	Use after free in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15968	N/A	A-OPE-BACK-181120/242
Use After Free	03-Nov-20	6.8	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15969	N/A	A-OPE-BACK-181120/243
Use After Free	03-Nov-20	6.8	Use after free in printing in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15971	N/A	A-OPE-BACK-181120/244
Use After Free	03-Nov-20	6.8	Use after free in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted	N/A	A-OPE-BACK-181120/245

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
			HTML page. CVE ID : CVE-2020-15972		
N/A	03-Nov-20	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 86.0.4240.75 allowed an attacker who convinced a user to install a malicious extension to bypass same origin policy via a crafted Chrome Extension. CVE ID : CVE-2020-15973	N/A	A-OPE-BACK-181120/246
N/A	03-Nov-20	4.6	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 86.0.4240.75 allowed a local attacker to bypass navigation restrictions via crafted Intents. CVE ID : CVE-2020-15980	N/A	A-OPE-BACK-181120/247
Use After Free	03-Nov-20	6.8	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted WebRTC stream. CVE ID : CVE-2020-15987	N/A	A-OPE-BACK-181120/248
Improper Initialization	03-Nov-20	4.3	Uninitialized data in PDFium in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file. CVE ID : CVE-2020-15989	N/A	A-OPE-BACK-181120/249

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
Use After Free	03-Nov-20	6.8	Use after free in PDFium in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. CVE ID : CVE-2020-16002	N/A	A-OPE-BACK-181120/250
Use After Free	03-Nov-20	6.8	Use after free in user interface in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16004	N/A	A-OPE-BACK-181120/251
Out-of-bounds Write	03-Nov-20	6.8	Insufficient policy enforcement in ANGLE in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16005	N/A	A-OPE-BACK-181120/252
Out-of-bounds Write	03-Nov-20	6.8	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16006	N/A	A-OPE-BACK-181120/253
Improper Input Validation	03-Nov-20	4.6	Insufficient data validation in installer in Google Chrome prior to 86.0.4240.183 allowed a local attacker to potentially elevate privilege	N/A	A-OPE-BACK-181120/254

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
			via a crafted filesystem. CVE ID : CVE-2020-16007		
Out-of-bounds Write	03-Nov-20	7.5	Stack buffer overflow in WebRTC in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit stack corruption via a crafted WebRTC packet. CVE ID : CVE-2020-16008	N/A	A-OPE-BACK-181120/255
Out-of-bounds Write	03-Nov-20	6.8	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16009	N/A	A-OPE-BACK-181120/256
Oracle					
fusion_middleware					
N/A	02-Nov-20	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8	N/A	A-ORA-FUSI-181120/257

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
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). CVE ID : CVE-2020-14750		
Osticket					
osticket					
Server-Side Request Forgery (SSRF)	02-Nov-20	7.5	SSRF exists in osTicket before 1.14.3, where an attacker can add malicious file to server or perform port scanning. CVE ID : CVE-2020-24881	N/A	A-OST-OSTI-181120/258
pega					
pega_platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-20	4.3	Pega Platform before 8.4.0 has a XSS issue via stream rule parameters used in the request header. CVE ID : CVE-2020-24353	N/A	A-PEG-PEGA-181120/259
Phpmyadmin					
phpmyadmin					
N/A	04-Nov-20	6.8	** DISPUTED ** phpMyAdmin through 5.0.2 allows CSV injection via Export Section. NOTE: the vendor disputes this because "the CSV file is accurately generated based on the database contents." CVE ID : CVE-2020-22278	N/A	A-PHP-PHPM-181120/260
protocol					

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
ipfs					
N/A	02-Nov-20	5	An issue was discovered in IPFS (aka go-ipfs) 0.4.23. An attacker can generate ephemeral identities (Sybils) and leverage the IPFS connection management reputation system to poison other nodes' routing tables, eclipsing the nodes that are the target of the attack from the rest of the network. Later versions, in particular go-ipfs 0.7, mitigate this. CVE ID : CVE-2020-10937	N/A	A-PRO-IPFS-181120/261
Qemu					
qemu					
Incorrect Calculation	06-Nov-20	4	ati_2d_blt in hw/display/ati_2d.c in QEMU 4.2.1 can encounter an outside-limits situation in a calculation. A guest can crash the QEMU process. CVE ID : CVE-2020-27616	http://www.openwall.com/lists/oss-security/2020/11/03/2	A-QEM-QEMU-181120/262
Reachable Assertion	06-Nov-20	4	eth_get_gso_type in net/eth.c in QEMU 4.2.1 allows guest OS users to trigger an assertion failure. A guest can crash the QEMU process via packet data that lacks a valid Layer 3 protocol. CVE ID : CVE-2020-27617	http://www.openwall.com/lists/oss-security/2020/11/02/1	A-QEM-QEMU-181120/263
robware					
rvtools					
Insufficiently Protected Credentials	05-Nov-20	5	RVToolsPasswordEncryption.exe in RVTools 4.0.6 allows users to encrypt passwords to be used in the	N/A	A-ROB-RVTO-181120/264

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
			configuration files. This encryption used a static IV and key, and thus using the Decrypt() method from VISKD.cs from the RVTools.exe executable allows for decrypting the encrypted passwords. The accounts used in the configuration files have access to vSphere instances. CVE ID : CVE-2020-27688		
SAP					
solution_manager					
Missing Authorization	10-Nov-20	6.4	SAP Solution Manager (JAVA stack), version - 7.20, allows an unauthenticated attacker to compromise the system because of missing authorization checks in the SVG Converter Service, this has an impact to the integrity and availability of the service. CVE ID : CVE-2020-26821	N/A	A-SAP-SOLU-181120/265
Missing Authorization	10-Nov-20	6.4	SAP Solution Manager (JAVA stack), version - 7.20, allows an unauthenticated attacker to compromise the system because of missing authorization checks in the Outside Discovery Configuration Service, this has an impact to the integrity and availability of the service. CVE ID : CVE-2020-26822	N/A	A-SAP-SOLU-181120/266
Missing Authorization	10-Nov-20	6.4	SAP Solution Manager (JAVA stack), version - 7.20, allows	N/A	A-SAP-SOLU-

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
n			an unauthenticated attacker to compromise the system because of missing authorization checks in the Upgrade Diagnostics Agent Connection Service, this has an impact to the integrity and availability of the service. CVE ID : CVE-2020-26823		181120/267
Missing Authorization	10-Nov-20	6.4	SAP Solution Manager (JAVA stack), version - 7.20, allows an unauthenticated attacker to compromise the system because of missing authorization checks in the Upgrade Legacy Ports Service, this has an impact to the integrity and availability of the service. CVE ID : CVE-2020-26824	N/A	A-SAP-SOLU-181120/268
netweaver_application_server_java					
Unrestricted Upload of File with Dangerous Type	10-Nov-20	9	SAP NetWeaver AS JAVA, versions - 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker who is authenticated as an administrator to use the administrator console, to expose unauthenticated access to the file system and upload a malicious file. The attacker or another user can then use a separate mechanism to execute OS commands through the uploaded file leading to Privilege Escalation and completely compromise the confidentiality, integrity and availability of the server	N/A	A-SAP-NETW-181120/269

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
			operating system and any application running on it. CVE ID : CVE-2020-26820		
sddm_project					
sddm					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Nov-20	3.3	An issue was discovered in SDDM before 0.19.0. It incorrectly starts the X server in a way that - for a short time period - allows local unprivileged users to create a connection to the X server without providing proper authentication. A local attacker can thus access X server display contents and, for example, intercept keystrokes or access the clipboard. This is caused by a race condition during Xauthority file creation. CVE ID : CVE-2020-28049	N/A	A-SDD-SDDM-181120/270
Silver-peak					
unity_orchestrator					
Improper Authentication	05-Nov-20	7.5	Silver Peak Unity Orchestrator versions prior to 8.9.11+, 8.10.11+, or 9.0.1+ uses HTTP headers to authenticate REST API calls from localhost. This makes it possible to log in to Orchestrator by introducing an HTTP HOST header set to 127.0.0.1 or localhost. Orchestrator instances that are hosted by customers – on-premise or in a public cloud provider – are affected	N/A	A-SIL-UNIT-181120/271

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
			by this vulnerability. CVE ID : CVE-2020-12145		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Nov-20	6.5	In Silver Peak Unity Orchestrator versions prior to 8.9.11+, 8.10.11+, or 9.0.1+, an authenticated user can access, modify, and delete restricted files on the Orchestrator server using the /debugFiles REST API. CVE ID : CVE-2020-12146	N/A	A-SIL-UNIT-181120/272
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Nov-20	6.5	In Silver Peak Unity Orchestrator versions prior to 8.9.11+, 8.10.11+, or 9.0.1+, an authenticated user can make unauthorized MySQL queries against the Orchestrator database using the /sqlExecution REST API, which had been used for internal testing. CVE ID : CVE-2020-12147	N/A	A-SIL-UNIT-181120/273
Tcpdump					
tcpdump					
N/A	04-Nov-20	7.5	The tok2strbuf() function in tcpdump 4.10.0-PRE-GIT was used by the SOME/IP dissector in an unsafe way. CVE ID : CVE-2020-8036	N/A	A-TCP-TCPD-181120/274
Allocation of Resources Without Limits or Throttling	04-Nov-20	5	The ppp decapsulator in tcpdump 4.9.3 can be convinced to allocate a large amount of memory. CVE ID : CVE-2020-8037	N/A	A-TCP-TCPD-181120/275
Telerik					
fiddler					

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
N/A	05-Nov-20	6.8	Telerik Fiddler through 5.0.20202.18177 allows attackers to execute arbitrary programs via a hostname with a trailing space character, followed by --utility-and-browser --utility-cmd-prefix= and the pathname of a locally installed program. The victim must interactively choose the Open On Browser option. Fixed in version 5.0.20204. CVE ID : CVE-2020-13661	N/A	A-TEL-FIDD-181120/276
web-audimex					
audimexee					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	3.5	AudimexEE before 14.1.1 is vulnerable to Reflected XSS (Cross-Site-Scripting). If the recommended security configuration parameter "unique_error_numbers" is not set, remote attackers can inject arbitrary web script or HTML via 'action, cargo, panel' parameters that can lead to data leakage. CVE ID : CVE-2020-28047	N/A	A-WEB-AUDI-181120/277
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Nov-20	6.5	SQL Injection vulnerability in "Documents component" found in AudimexEE version 14.1.0 allows an attacker to execute arbitrary SQL commands via the object_path parameter. CVE ID : CVE-2020-28115	N/A	A-WEB-AUDI-181120/278
weformspro					

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
weforms					
N/A	04-Nov-20	7.5	WeForms Wordpress Plugin 1.4.7 allows CSV injection via a form's entry. CVE ID : CVE-2020-22276	N/A	A-WEF-WEFO-181120/279
whatsapp					
whatsapp					
Files or Directories Accessible to External Parties	03-Nov-20	2.1	Improper authorization of the Screen Lock feature in WhatsApp and WhatsApp Business for iOS prior to v2.20.100 could have permitted use of Siri to interact with the WhatsApp application even after the phone was locked. CVE ID : CVE-2020-1908	https://www.whatsapp.com/security/advisories/2020/	A-WHA-WHAT-181120/280
Use After Free	03-Nov-20	7.5	A use-after-free in a logging library in WhatsApp for iOS prior to v2.20.111 and WhatsApp Business for iOS prior to v2.20.111 could have resulted in memory corruption, crashes and potentially code execution. This could have happened only if several events occurred together in sequence, including receiving an animated sticker while placing a WhatsApp video call on hold. CVE ID : CVE-2020-1909	https://www.whatsapp.com/security/advisories/2020/	A-WHA-WHAT-181120/281
whatsapp_business					
Files or Directories Accessible to External	03-Nov-20	2.1	Improper authorization of the Screen Lock feature in WhatsApp and WhatsApp Business for iOS prior to	https://www.whatsapp.com/security/advisories/2020/	A-WHA-WHAT-181120/282

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
Parties			v2.20.100 could have permitted use of Siri to interact with the WhatsApp application even after the phone was locked. CVE ID : CVE-2020-1908	visories/2020/	
Use After Free	03-Nov-20	7.5	A use-after-free in a logging library in WhatsApp for iOS prior to v2.20.111 and WhatsApp Business for iOS prior to v2.20.111 could have resulted in memory corruption, crashes and potentially code execution. This could have happened only if several events occurred together in sequence, including receiving an animated sticker while placing a WhatsApp video call on hold. CVE ID : CVE-2020-1909	https://www.whatsapp.com/security/advisories/2020/	A-WHA-WHAT-181120/283
Wireshark					
wireshark					
Uncontrolled Resource Consumption	02-Nov-20	5	In Wireshark 3.2.0 to 3.2.7, the GQUIC dissector could crash. This was addressed in epan/dissectors/packet-gquic.c by correcting the implementation of offset advancement. CVE ID : CVE-2020-28030	N/A	A-WIR-WIRE-181120/284
Wordpress					
wordpress					
Deserialization of Untrusted Data	02-Nov-20	7.5	WordPress before 5.5.2 mishandles deserialization requests in wp-includes/Requests/Utility/Fi	N/A	A-WOR-WORD-181120/285

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
			IteratedIterator.php. CVE ID : CVE-2020-28032		
N/A	02-Nov-20	5	WordPress before 5.5.2 mishandles embeds from disabled sites on a multisite network, as demonstrated by allowing a spam embed. CVE ID : CVE-2020-28033	N/A	A-WOR-WORD-181120/286
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-20	4.3	WordPress before 5.5.2 allows XSS associated with global variables. CVE ID : CVE-2020-28034	N/A	A-WOR-WORD-181120/287
Improper Privilege Management	02-Nov-20	7.5	WordPress before 5.5.2 allows attackers to gain privileges via XML-RPC. CVE ID : CVE-2020-28035	N/A	A-WOR-WORD-181120/288
Improper Privilege Management	02-Nov-20	7.5	wp-includes/class-wp-xmlrpc-server.php in WordPress before 5.5.2 allows attackers to gain privileges by using XML-RPC to comment on a post. CVE ID : CVE-2020-28036	N/A	A-WOR-WORD-181120/289
Improper Input Validation	02-Nov-20	7.5	is_blog_installed in wp-includes/functions.php in WordPress before 5.5.2 improperly determines whether WordPress is already installed, which might allow an attacker to perform a new installation, leading to remote code execution (as well as a denial of service for the old	N/A	A-WOR-WORD-181120/290

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
			installation). CVE ID : CVE-2020-28037		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-20	4.3	WordPress before 5.5.2 allows stored XSS via post slugs. CVE ID : CVE-2020-28038	N/A	A-WOR-WORD-181120/291
N/A	02-Nov-20	6.4	is_protected_meta in wp-includes/meta.php in WordPress before 5.5.2 allows arbitrary file deletion because it does not properly determine whether a meta key is considered protected. CVE ID : CVE-2020-28039	N/A	A-WOR-WORD-181120/292
Cross-Site Request Forgery (CSRF)	02-Nov-20	4.3	WordPress before 5.5.2 allows CSRF attacks that change a theme's background image. CVE ID : CVE-2020-28040	N/A	A-WOR-WORD-181120/293
Operating System					
Apple					
mac_os					
Out-of-bounds Read	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as	N/A	O-APP-MAC_-181120/294

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
			ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24426		
Improper Input Validation	05-Nov-20	4.3	Acrobat Reader versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an input validation vulnerability when decoding a crafted codec that could result in the disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24427	N/A	O-APP-MAC_-181120/295
Time-of-check Time-of-use (TOCTOU) Race Condition	05-Nov-20	5.1	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a time-of-check time-of-use (TOCTOU) race condition vulnerability that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24428	N/A	O-APP-MAC_-181120/296

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
Improper Verification of Cryptographic Signature	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a signature verification bypass that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24429	N/A	O-APP-MAC_-181120/297
Use After Free	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability when handling malicious JavaScript. This vulnerability could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24430	N/A	O-APP-MAC_-181120/298
Improper Authorization	05-Nov-20	5.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a security feature bypass that could result in dynamic library code injection by the Adobe	N/A	O-APP-MAC_-181120/299

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
			Reader process. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24431		
Improper Input Validation	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) and Adobe Acrobat Pro DC 2017.011.30175 (and earlier) are affected by an improper input validation vulnerability that could result in arbitrary JavaScript execution in the context of the current user. To exploit this issue, an attacker must acquire and then modify a certified PDF document that is trusted by the victim. The attacker then needs to convince the victim to open the document. CVE ID : CVE-2020-24432	N/A	O-APP-MAC_-181120/300
Improper Access Control	05-Nov-20	9.3	Adobe Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a local privilege escalation vulnerability that could enable a user without administrator privileges to delete arbitrary files and potentially execute arbitrary code as SYSTEM. Exploitation of this issue	N/A	O-APP-MAC_-181120/301

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
			requires an attacker to socially engineer a victim, or the attacker must already have some access to the environment. CVE ID : CVE-2020-24433		
Out-of-bounds Read	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24434	N/A	O-APP-MAC_-181120/302
Heap-based Buffer Overflow	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a heap-based buffer overflow vulnerability in the submitForm function, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file in Acrobat Reader.	N/A	O-APP-MAC_-181120/303

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
			CVE ID : CVE-2020-24435		
Out-of-bounds Write	05-Nov-20	6.8	<p>Acrobat Pro DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds write vulnerability that could result in writing past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. This vulnerability requires user interaction to exploit in that the victim must open a malicious document.</p> <p>CVE ID : CVE-2020-24436</p>	N/A	O-APP-MAC_-181120/304
Use After Free	05-Nov-20	6.8	<p>Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2020-24437</p>	N/A	O-APP-MAC_-181120/305
Use After Free	05-Nov-20	4.3	<p>Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005</p>	N/A	O-APP-MAC_-181120/306

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
			(and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability that could result in a memory address leak. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24438		
iphone_os					
N/A	03-Nov-20	4.3	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 86.0.4240.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted URL. CVE ID : CVE-2020-15984	N/A	O-APP-IPHO-181120/307
mac_os_x					
Improper Input Validation	03-Nov-20	4.3	Insufficient data validation in dialogs in Google Chrome on OS X prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page. CVE ID : CVE-2020-15977	N/A	O-APP-MAC_-181120/308
Canonical					
ubuntu_linux					
Incorrect Permission Assignment for Critical Resource	06-Nov-20	4.6	Ubuntu's packaging of libvirt in 20.04 LTS created a control socket with world read and write permissions. An attacker could use this to overwrite arbitrary files or	N/A	O-CAN-UBUN-181120/309

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
			execute arbitrary code. CVE ID : CVE-2020-15708		
Debian					
debian_linux					
Allocation of Resources Without Limits or Throttling	04-Nov-20	5	The ppp decapsulator in tcpdump 4.9.3 can be convinced to allocate a large amount of memory. CVE ID : CVE-2020-8037	N/A	O-DEB-DEBI-181120/310
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Nov-20	3.3	An issue was discovered in SDDM before 0.19.0. It incorrectly starts the X server in a way that - for a short time period - allows local unprivileged users to create a connection to the X server without providing proper authentication. A local attacker can thus access X server display contents and, for example, intercept keystrokes or access the clipboard. This is caused by a race condition during Xauthority file creation. CVE ID : CVE-2020-28049	N/A	O-DEB-DEBI-181120/311
Fedoraproject					
fedora					
Use After Free	03-Nov-20	6.8	Use after free in payments in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15967	N/A	O-FED-FEDO-181120/312

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
Use After Free	03-Nov-20	6.8	Use after free in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15968	N/A	O-FED-FEDO-181120/313
Use After Free	03-Nov-20	6.8	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15969	N/A	O-FED-FEDO-181120/314
Use After Free	03-Nov-20	6.8	Use after free in NFC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15970	N/A	O-FED-FEDO-181120/315
Use After Free	03-Nov-20	6.8	Use after free in printing in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15971	N/A	O-FED-FEDO-181120/316
Use After Free	03-Nov-20	6.8	Use after free in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap	N/A	O-FED-FEDO-181120/317

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
			corruption via a crafted HTML page. CVE ID : CVE-2020-15972		
N/A	03-Nov-20	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 86.0.4240.75 allowed an attacker who convinced a user to install a malicious extension to bypass same origin policy via a crafted Chrome Extension. CVE ID : CVE-2020-15973	N/A	O-FED-FEDO-181120/318
N/A	03-Nov-20	4.6	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 86.0.4240.75 allowed a local attacker to bypass navigation restrictions via crafted Intents. CVE ID : CVE-2020-15980	N/A	O-FED-FEDO-181120/319
Out-of-bounds Read	03-Nov-20	4.3	Out of bounds read in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. CVE ID : CVE-2020-15981	N/A	O-FED-FEDO-181120/320
N/A	03-Nov-20	4.3	Inappropriate implementation in cache in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML	N/A	O-FED-FEDO-181120/321

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
			page. CVE ID : CVE-2020-15982		
Improper Input Validation	03-Nov-20	4.4	Insufficient data validation in webUI in Google Chrome on ChromeOS prior to 86.0.4240.75 allowed a local attacker to bypass content security policy via a crafted HTML page. CVE ID : CVE-2020-15983	N/A	O-FED-FEDO-181120/322
N/A	03-Nov-20	4.3	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 86.0.4240.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted URL. CVE ID : CVE-2020-15984	N/A	O-FED-FEDO-181120/323
N/A	03-Nov-20	4.3	Inappropriate implementation in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to spoof security UI via a crafted HTML page. CVE ID : CVE-2020-15985	N/A	O-FED-FEDO-181120/324
Use After Free	03-Nov-20	4.3	Integer overflow in media in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15986	N/A	O-FED-FEDO-181120/325
Use After Free	03-Nov-20	6.8	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to	N/A	O-FED-FEDO-181120/326

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
			potentially exploit heap corruption via a crafted WebRTC stream. CVE ID : CVE-2020-15987		
N/A	03-Nov-20	6.8	Insufficient policy enforcement in downloads in Google Chrome on Windows prior to 86.0.4240.75 allowed a remote attacker who convinced the user to open files to execute arbitrary code via a crafted HTML page. CVE ID : CVE-2020-15988	N/A	O-FED-FEDO-181120/327
Improper Initialization	03-Nov-20	4.3	Uninitialized data in PDFium in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file. CVE ID : CVE-2020-15989	N/A	O-FED-FEDO-181120/328
Use After Free	03-Nov-20	6.8	Use after free in PDFium in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. CVE ID : CVE-2020-16002	N/A	O-FED-FEDO-181120/329
Google					
android					
Incorrect Default Permissions	10-Nov-20	2.1	In CellBroadcastReceiver's intent handlers, there is a possible denial of service due to a missing permission	N/A	O-GOO-ANDR-181120/330

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
			check. This could lead to local denial of service of emergency alerts with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-162741784 CVE ID : CVE-2020-0437		
Improper Initialization	10-Nov-20	4.6	In the AIBinder_Class constructor of ibinder.cpp, there is a possible arbitrary code execution due to uninitialized data. This could lead to local escalation of privilege if a process were using libbinder_ndk in a vulnerable way with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-161812320 CVE ID : CVE-2020-0438	N/A	O-GOO-ANDR-181120/331
Incorrect Default Permissions	10-Nov-20	4.6	In generatePackageInfo of PackageManagerService.java , there is a possible permissions bypass due to an incorrect permission check. This could lead to local escalation of privilege that allows instant apps access to permissions not allowed for instant apps, with no additional execution	N/A	O-GOO-ANDR-181120/332

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
			<p>privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0 Android ID: A-140256621</p> <p>CVE ID : CVE-2020-0439</p>		
Uncontrolled Resource Consumption	10-Nov-20	7.8	<p>In Message and toBundle of Notification.java, there is a possible resource exhaustion due to improper input validation. This could lead to remote denial of service requiring a device reset to fix with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-11 Android-8.0 Android-8.1 Android-9 Android-10 Android ID: A-158304295</p> <p>CVE ID : CVE-2020-0441</p>	N/A	O-GOO-ANDR-181120/333
Improper Input Validation	10-Nov-20	7.8	<p>In Message and toBundle of Notification.java, there is a possible UI slowdown or crash due to improper input validation. This could lead to remote denial of service if a malicious contact file is received, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-10 Android-11 Android-8.0</p>	N/A	O-GOO-ANDR-181120/334

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
			Android-8.1 Android-9 Android ID: A-147358092 CVE ID : CVE-2020-0442		
Improper Check for Unusual or Exceptional Conditions	10-Nov-20	2.1	In LocaleList of LocaleList.java, there is a possible forced reboot due to an uncaught exception. This could lead to local denial of service requiring factory reset to restore with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-152410253 CVE ID : CVE-2020-0443	N/A	O-GOO-ANDR-181120/335
N/A	10-Nov-20	7.5	There is a possible out of bounds write due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-168264527 CVE ID : CVE-2020-0445	N/A	O-GOO-ANDR-181120/336
N/A	10-Nov-20	7.5	There is a possible out of bounds write due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-168264528 CVE ID : CVE-2020-0446	N/A	O-GOO-ANDR-181120/337
N/A	10-Nov-20	7.5	There is a possible out of bounds write due to a missing bounds check.Product:	N/A	O-GOO-ANDR-181120/338

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
			AndroidVersions: Android SoCAndroid ID: A- 168251617 CVE ID : CVE-2020-0447		
Incorrect Default Permissions	10-Nov-20	2.1	In getPhoneAccountsForPackag e of TelecomServiceImpl.java, there is a possible way to access a tracking identifier due to a missing permission check. This could lead to local information disclosure of the identifier, which could be used to track an account across devices, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android- 8.0 Android-8.1 Android-9 Android-10 Android- 11Android ID: A-153995334 CVE ID : CVE-2020-0448	N/A	O-GOO-ANDR- 181120/339
Use After Free	10-Nov-20	9.3	In btm_sec_disconnected of btm_sec.cc, there is a possible memory corruption due to a use after free. This could lead to remote code execution in the Bluetooth server with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.0 Android- 8.1Android ID: A- 162497143	N/A	O-GOO-ANDR- 181120/340

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
			CVE ID : CVE-2020-0449		
Improper Initialization	10-Nov-20	4.3	In rw_i93_sm_format of rw_i93.cc, there is a possible out of bounds read due to uninitialized data. This could lead to remote information disclosure over NFC with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-157650336 CVE ID : CVE-2020-0450	N/A	O-GOO-ANDR-181120/341
Out-of-bounds Write	10-Nov-20	9.3	In sbrDecoder_AssignQmfChannels2SbrChannels of sbrdecoder.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9 Android-8.0 Android-8.1Android ID: A-158762825 CVE ID : CVE-2020-0451	N/A	O-GOO-ANDR-181120/342
Integer Overflow or Wraparound	10-Nov-20	7.5	In exif_entry_get_value of exif-entry.c, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution if a third	N/A	O-GOO-ANDR-181120/343

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
			party app used this library to process remote image data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-159625731 CVE ID : CVE-2020-0452		
Incorrect Default Permissions	10-Nov-20	2.1	In updateNotification of BeamTransferManager.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-8.0 Android-8.1Android ID: A-159060474 CVE ID : CVE-2020-0453	N/A	O-GOO-ANDR-181120/344
Incorrect Permission Assignment for Critical Resource	10-Nov-20	2.1	In callCallbackForRequest of ConnectivityService.java, there is a possible permission bypass due to a missing permission check. This could lead to local information disclosure of the current SSID with User execution privileges needed. User interaction is not needed for exploitation.Product:	N/A	O-GOO-ANDR-181120/345

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
			AndroidVersions: Android-9 Android ID: A-161370134 CVE ID : CVE-2020-0454		
Use After Free	03-Nov-20	6.8	Use after free in WebXR in Google Chrome on Android prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15976	N/A	O-GOO-ANDR-181120/346
Improper Input Validation	03-Nov-20	6.8	Insufficient data validation in navigation in Google Chrome on Android prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. CVE ID : CVE-2020-15978	N/A	O-GOO-ANDR-181120/347
N/A	03-Nov-20	4.6	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 86.0.4240.75 allowed a local attacker to bypass navigation restrictions via crafted Intents. CVE ID : CVE-2020-15980	N/A	O-GOO-ANDR-181120/348
Use After Free	03-Nov-20	6.8	Use after free in printing in Google Chrome prior to 86.0.4240.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15993	N/A	O-GOO-ANDR-181120/349

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
Use After Free	03-Nov-20	6.8	Use after free in V8 in Google Chrome prior to 86.0.4240.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15994	N/A	O-GOO-ANDR-181120/350
Out-of-bounds Write	03-Nov-20	6.8	Out of bounds write in V8 in Google Chrome prior to 86.0.4240.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-15995	N/A	O-GOO-ANDR-181120/351
Use After Free	03-Nov-20	6.8	Use after free in passwords in Google Chrome prior to 86.0.4240.99 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15996	N/A	O-GOO-ANDR-181120/352
Use After Free	03-Nov-20	6.8	Use after free in Mojo in Google Chrome prior to 86.0.4240.99 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15997	N/A	O-GOO-ANDR-181120/353
Use After Free	03-Nov-20	6.8	Use after free in USB in Google Chrome prior to 86.0.4240.99 allowed a remote attacker who had compromised the renderer	N/A	O-GOO-ANDR-181120/354

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
			process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-15998		
Out-of-bounds Write	03-Nov-20	6.8	Heap buffer overflow in UI in Google Chrome on Android prior to 86.0.4240.185 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-16010	N/A	O-GOO-ANDR-181120/355
N/A	08-Nov-20	7.5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) software. Attackers can bypass Factory Reset Protection (FRP) via Secure Folder. The Samsung ID is SVE-2020-18546 (November 2020). CVE ID : CVE-2020-28340	N/A	O-GOO-ANDR-181120/356
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Nov-20	4.6	An issue was discovered on Samsung mobile devices with Q(10.0) (Exynos990 chipsets) software. The S3K250AF Secure Element CC EAL 5+ chip allows attackers to execute arbitrary code and obtain sensitive information via a buffer overflow. The Samsung ID is SVE-2020-18632 (November 2020). CVE ID : CVE-2020-28341	N/A	O-GOO-ANDR-181120/357
N/A	08-Nov-20	6.8	An issue was discovered on Samsung mobile devices	N/A	O-GOO-ANDR-

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
			with P(9.0) and Q(10.0) (China / India) software. The S Secure application allows attackers to bypass authentication for a locked Gallery application via the Reminder application. The Samsung ID is SVE-2020-18689 (November 2020). CVE ID : CVE-2020-28342		181120/358
Out-of-bounds Write	08-Nov-20	4.6	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 980, 9820, and 9830 chipsets) software. The NPU driver allows attackers to execute arbitrary code because of unintended write and read operations on memory. The Samsung ID is SVE-2020-18610 (November 2020). CVE ID : CVE-2020-28343	N/A	O-GOO-ANDR-181120/359
imomobile					
verve_connect_vh510_firmware					
Use of Hard-coded Credentials	04-Nov-20	5	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 contains undocumented default admin credentials for the web management interface. A remote attacker could exploit this vulnerability to login and execute commands on the device, as well as upgrade the firmware image to a malicious version. CVE ID : CVE-2020-27689	N/A	O-IMO-VERV-181120/360

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Nov-20	4.9	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 contains a buffer overflow within its web management portal. When a POST request is sent to /boaform/admin/formDOM AINBLK with a large blkDomain value, the Boa server crashes. CVE ID : CVE-2020-27690	N/A	O-IMO-VERV-181120/361
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-20	4.3	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 allows XSS via URLBlocking Settings, SNMP Settings, and System Log Settings. CVE ID : CVE-2020-27691	N/A	O-IMO-VERV-181120/362
Cross-Site Request Forgery (CSRF)	04-Nov-20	6.8	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 contains multiple CSRF vulnerabilities within its web management portal. Attackers can, for example, use this to update the TR-069 configuration server settings (responsible for managing devices remotely). This makes it possible to remotely reboot the device or upload malicious firmware. CVE ID : CVE-2020-27692	N/A	O-IMO-VERV-181120/363
Microsoft					
windows					
N/A	03-Nov-20	6.8	Insufficient policy enforcement in downloads	N/A	O-MIC-WIND-181120/364

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
			in Google Chrome on Windows prior to 86.0.4240.75 allowed a remote attacker who convinced the user to open files to execute arbitrary code via a crafted HTML page. CVE ID : CVE-2020-15988		
Out-of-bounds Write	03-Nov-20	7.5	Heap buffer overflow in UI in Google Chrome on Windows prior to 86.0.4240.183 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2020-16011	N/A	O-MIC-WIND-181120/365
Out-of-bounds Read	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24426	N/A	O-MIC-WIND-181120/366
Improper Input Validation	05-Nov-20	4.3	Acrobat Reader versions 2020.012.20048 (and earlier), 2020.001.30005	N/A	O-MIC-WIND-181120/367

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
			(and earlier) and 2017.011.30175 (and earlier) are affected by an input validation vulnerability when decoding a crafted codec that could result in the disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24427		
Time-of-check Time-of-use (TOCTOU) Race Condition	05-Nov-20	5.1	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a time-of-check time-of-use (TOCTOU) race condition vulnerability that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24428	N/A	O-MIC-WIND-181120/368
Improper Verification of Cryptographic Signature	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a signature verification bypass that could result in local privilege	N/A	O-MIC-WIND-181120/369

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
			escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24429		
Use After Free	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability when handling malicious JavaScript. This vulnerability could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24430	N/A	O-MIC-WIND-181120/370
Improper Authorization	05-Nov-20	5.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a security feature bypass that could result in dynamic library code injection by the Adobe Reader process. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24431	N/A	O-MIC-WIND-181120/371
Improper Input Validation	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005	N/A	O-MIC-WIND-181120/372

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
			(and earlier) and 2017.011.30175 (and earlier) and Adobe Acrobat Pro DC 2017.011.30175 (and earlier) are affected by an improper input validation vulnerability that could result in arbitrary JavaScript execution in the context of the current user. To exploit this issue, an attacker must acquire and then modify a certified PDF document that is trusted by the victim. The attacker then needs to convince the victim to open the document. CVE ID : CVE-2020-24432		
Improper Access Control	05-Nov-20	9.3	Adobe Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a local privilege escalation vulnerability that could enable a user without administrator privileges to delete arbitrary files and potentially execute arbitrary code as SYSTEM. Exploitation of this issue requires an attacker to socially engineer a victim, or the attacker must already have some access to the environment. CVE ID : CVE-2020-24433	N/A	O-MIC-WIND-181120/373
Out-of-bounds Read	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and	N/A	O-MIC-WIND-181120/374

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
			earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24434		
Heap-based Buffer Overflow	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a heap-based buffer overflow vulnerability in the submitForm function, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file in Acrobat Reader. CVE ID : CVE-2020-24435	N/A	O-MIC-WIND-181120/375
Out-of-bounds Write	05-Nov-20	6.8	Acrobat Pro DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds write vulnerability that could	N/A	O-MIC-WIND-181120/376

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
			result in writing past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. This vulnerability requires user interaction to exploit in that the victim must open a malicious document. CVE ID : CVE-2020-24436		
Use After Free	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2020-24437	N/A	O-MIC-WIND-181120/377
Use After Free	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability that could result in a memory address leak. Exploitation of this issue requires user interaction in that a victim must open a	N/A	O-MIC-WIND-181120/378

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
			malicious file. CVE ID : CVE-2020-24438		
windows_10					
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17025	N/A	O-MIC-WIND-181120/379
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17026	N/A	O-MIC-WIND-181120/380
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055.	N/A	O-MIC-WIND-181120/381

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
			CVE ID : CVE-2020-17027		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17028	N/A	O-MIC-WIND-181120/382
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17031	N/A	O-MIC-WIND-181120/383
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17032	N/A	O-MIC-WIND-181120/384
Improper Privilege	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege	N/A	O-MIC-WIND-181120/385

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
Management			Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17033		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17034	N/A	O-MIC-WIND-181120/386
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17043	N/A	O-MIC-WIND-181120/387
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026,	N/A	O-MIC-WIND-181120/388

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
			CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17055. CVE ID : CVE-2020-17044		
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044. CVE ID : CVE-2020-17055	N/A	O-MIC-WIND-181120/389
windows_7					
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17043	N/A	O-MIC-WIND-181120/390
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031,	N/A	O-MIC-WIND-181120/391

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
			CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17055. CVE ID : CVE-2020-17044		
windows_8.1					
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17025	N/A	O-MIC-WIND-181120/392
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17026	N/A	O-MIC-WIND-181120/393
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043,	N/A	O-MIC-WIND-181120/394

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
			CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17027		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17028	N/A	O-MIC-WIND-181120/395
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17031	N/A	O-MIC-WIND-181120/396
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17032	N/A	O-MIC-WIND-181120/397

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
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17033	N/A	O-MIC-WIND-181120/398
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17034	N/A	O-MIC-WIND-181120/399
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17043	N/A	O-MIC-WIND-181120/400
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is	N/A	O-MIC-WIND-181120/401

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
			unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17055. CVE ID : CVE-2020-17044		
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044. CVE ID : CVE-2020-17055	N/A	O-MIC-WIND-181120/402
windows_rt_8.1					
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17025	N/A	O-MIC-WIND-181120/403
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17027,	N/A	O-MIC-WIND-181120/404

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
			CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17026		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17027	N/A	O-MIC-WIND-181120/405
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17028	N/A	O-MIC-WIND-181120/406
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17032, CVE-2020-17033, CVE-2020-	N/A	O-MIC-WIND-181120/407

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
			17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17031		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17032	N/A	O-MIC-WIND-181120/408
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17033	N/A	O-MIC-WIND-181120/409
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055.	N/A	O-MIC-WIND-181120/410

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
			CVE ID : CVE-2020-17034		
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17043	N/A	O-MIC-WIND-181120/411
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17055. CVE ID : CVE-2020-17044	N/A	O-MIC-WIND-181120/412
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044. CVE ID : CVE-2020-17055	N/A	O-MIC-WIND-181120/413
windows_server_2008					

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
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17043	N/A	O-MIC-WIND-181120/414
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17055. CVE ID : CVE-2020-17044	N/A	O-MIC-WIND-181120/415
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044. CVE ID : CVE-2020-17055	N/A	O-MIC-WIND-181120/416
windows_server_2012					
Improper Privilege	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege	N/A	O-MIC-WIND-181120/417

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
Management			Vulnerability This CVE ID is unique from CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17025		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17026	N/A	O-MIC-WIND-181120/418
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17027	N/A	O-MIC-WIND-181120/419
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026,	N/A	O-MIC-WIND-181120/420

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
			CVE-2020-17027, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17028		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17031	N/A	O-MIC-WIND-181120/421
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17032	N/A	O-MIC-WIND-181120/422
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-	N/A	O-MIC-WIND-181120/423

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
			17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17033		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17034	N/A	O-MIC-WIND-181120/424
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17043	N/A	O-MIC-WIND-181120/425
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17055.	N/A	O-MIC-WIND-181120/426

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
			CVE ID : CVE-2020-17044		
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044. CVE ID : CVE-2020-17055	N/A	O-MIC-WIND-181120/427
windows_server_2016					
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17025	N/A	O-MIC-WIND-181120/428
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17026	N/A	O-MIC-WIND-181120/429

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
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17027	N/A	O-MIC-WIND-181120/430
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17028	N/A	O-MIC-WIND-181120/431
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17031	N/A	O-MIC-WIND-181120/432
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is	N/A	O-MIC-WIND-181120/433

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
			unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17032		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17033	N/A	O-MIC-WIND-181120/434
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17034	N/A	O-MIC-WIND-181120/435
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-	N/A	O-MIC-WIND-181120/436

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
			17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17043		
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17055. CVE ID : CVE-2020-17044	N/A	O-MIC-WIND-181120/437
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044. CVE ID : CVE-2020-17055	N/A	O-MIC-WIND-181120/438
windows_server_2019					
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-	N/A	O-MIC-WIND-181120/439

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
			17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17025		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17026	N/A	O-MIC-WIND-181120/440
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17027	N/A	O-MIC-WIND-181120/441
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055.	N/A	O-MIC-WIND-181120/442

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
			CVE ID : CVE-2020-17028		
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17031	N/A	O-MIC-WIND-181120/443
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17032	N/A	O-MIC-WIND-181120/444
Improper Privilege Management	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17033	N/A	O-MIC-WIND-181120/445
Improper Privilege	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege	N/A	O-MIC-WIND-181120/446

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
Management			Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17043, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17034		
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17044, CVE-2020-17055. CVE ID : CVE-2020-17043	N/A	O-MIC-WIND-181120/447
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026, CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17055. CVE ID : CVE-2020-17044	N/A	O-MIC-WIND-181120/448
Improper Privilege Management	11-Nov-20	6.8	Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17025, CVE-2020-17026,	N/A	O-MIC-WIND-181120/449

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
			CVE-2020-17027, CVE-2020-17028, CVE-2020-17031, CVE-2020-17032, CVE-2020-17033, CVE-2020-17034, CVE-2020-17043, CVE-2020-17044. CVE ID : CVE-2020-17055		
Mitsubishielectric					
melsec_iq-rj71eip91_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	7.5	Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5653	N/A	O-MIT-MELS-181120/450
Session Fixation	02-Nov-20	5	Session fixation vulnerability in TCP/IP function included	N/A	O-MIT-MELS-181120/451

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
			<p>in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5654</p>		
NULL Pointer Dereference	02-Nov-20	5	<p>NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before,</p>	N/A	O-MIT-MELS-181120/452

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
			RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5655		
N/A	02-Nov-20	7.5	Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	N/A	O-MIT-MELS-181120/453

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
			CVE ID : CVE-2020-5656		
Argument Injection or Modification	02-Nov-20	3.3	Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5657	N/A	O-MIT-MELS-181120/454
Uncontrolled Resource Consumption	02-Nov-20	5	Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are	N/A	O-MIT-MELS-181120/455

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
			'02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5658		
melsec_iq-rj71pn92_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	7.5	Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC	N/A	O-MIT-MELS-181120/456

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
			UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5653		
Session Fixation	02-Nov-20	5	Session fixation vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5654	N/A	O-MIT-MELS-181120/457
NULL Pointer Dereference	02-Nov-20	5	NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R	N/A	O-MIT-MELS-181120/458

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
			<p>series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5655</p>		
N/A	02-Nov-20	7.5	<p>Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface</p>	N/A	O-MIT-MELS-181120/459

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
			Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5656		
Argument Injection or Modification	02-Nov-20	3.3	Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially	N/A	O-MIT-MELS-181120/460

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
			crafted packet. CVE ID : CVE-2020-5657		
Uncontrolled Resource Consumption	02-Nov-20	5	Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5658	N/A	O-MIT-MELS-181120/461
melsec_iq-rd81dl96_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	7.5	Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller	N/A	O-MIT-MELS-181120/462

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
			Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5653		
Session Fixation	02-Nov-20	5	Session fixation vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a	N/A	O-MIT-MELS-181120/463

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
			remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5654		
NULL Pointer Dereference	02-Nov-20	5	NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5655	N/A	O-MIT-MELS-181120/464
N/A	02-Nov-20	7.5	Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2	N/A	O-MIT-MELS-181120/465

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
			<p>digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5656</p>		
Argument Injection or Modification	02-Nov-20	3.3	<p>Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface</p>	N/A	O-MIT-MELS-181120/466

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
			<p>Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5657</p>		
Uncontrolled Resource Consumption	02-Nov-20	5	<p>Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5658</p>	N/A	O-MIT-MELS-181120/467

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
melsec_iq-rd81mes96n_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	7.5	Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5653	N/A	O-MIT-MELS-181120/468
Session Fixation	02-Nov-20	5	Session fixation vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or	N/A	O-MIT-MELS-181120/469

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
			<p>before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5654</p>		
NULL Pointer Dereference	02-Nov-20	5	<p>NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network</p>	N/A	O-MIT-MELS-181120/470

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
			functions of the products via a specially crafted packet. CVE ID : CVE-2020-5655		
N/A	02-Nov-20	7.5	Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5656	N/A	O-MIT-MELS-181120/471
Argument Injection or Modification	02-Nov-20	3.3	Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network	N/A	O-MIT-MELS-181120/472

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
			<p>Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5657</p>		
Uncontrolled Resource Consumption	02-Nov-20	5	<p>Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of</p>	N/A	O-MIT-MELS-181120/473

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
			serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5658		
melsec_iq-rd81opc96_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	7.5	Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5653	N/A	O-MIT-MELS-181120/474

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
Session Fixation	02-Nov-20	5	<p>Session fixation vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5654</p>	N/A	O-MIT-MELS-181120/475
NULL Pointer Dereference	02-Nov-20	5	<p>NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module</p>	N/A	O-MIT-MELS-181120/476

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
			First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5655		
N/A	02-Nov-20	7.5	Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program	N/A	O-MIT-MELS-181120/477

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
			via a specially crafted packet. CVE ID : CVE-2020-5656		
Argument Injection or Modification	02-Nov-20	3.3	Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5657	N/A	O-MIT-MELS-181120/478
Uncontrolled Resource Consumption	02-Nov-20	5	Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2	N/A	O-MIT-MELS-181120/479

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
			digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5658		
Moxa					
vport_461_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Nov-20	10	A command injection vulnerability exists in Moxa Inc VPort 461 Series Firmware Version 3.4 or lower that could allow a remote attacker to execute arbitrary commands in Moxa's VPort 461 Series Industrial Video Servers. CVE ID : CVE-2020-23639	N/A	O-MOX-VPOR-181120/480
Opensuse					
leap					
Use After Free	03-Nov-20	6.8	Use after free in user interface in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to	N/A	O-OPE-LEAP-181120/481

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
			potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16004		
Out-of-bounds Write	03-Nov-20	6.8	Insufficient policy enforcement in ANGLE in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16005	N/A	O-OPE-LEAP-181120/482
Out-of-bounds Write	03-Nov-20	6.8	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16006	N/A	O-OPE-LEAP-181120/483
Improper Input Validation	03-Nov-20	4.6	Insufficient data validation in installer in Google Chrome prior to 86.0.4240.183 allowed a local attacker to potentially elevate privilege via a crafted filesystem. CVE ID : CVE-2020-16007	N/A	O-OPE-LEAP-181120/484
Out-of-bounds Write	03-Nov-20	7.5	Stack buffer overflow in WebRTC in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit stack corruption via a crafted WebRTC packet. CVE ID : CVE-2020-16008	N/A	O-OPE-LEAP-181120/485
Out-of-	03-Nov-20	6.8	Inappropriate	N/A	O-OPE-LEAP-

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
bounds Write			implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2020-16009		181120/486
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Nov-20	3.3	An issue was discovered in SDDM before 0.19.0. It incorrectly starts the X server in a way that - for a short time period - allows local unprivileged users to create a connection to the X server without providing proper authentication. A local attacker can thus access X server display contents and, for example, intercept keystrokes or access the clipboard. This is caused by a race condition during Xauthority file creation. CVE ID : CVE-2020-28049	N/A	O-OPE-LEAP-181120/487
Qualcomm					
qca6574au_firmware					
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/488

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
			Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/489

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
			QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/490

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
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/491
Buffer Copy without Checking Size of Input ('Classic	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered	https://www.qualcomm.com/company/product-	O-QUA-QCA6-181120/492

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
Buffer Overflow')			client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	security/bulletins/october-2020-bulletin	
qcs405_firmware					
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/493

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/494

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/495

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
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/496

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
			IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/497

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
			QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/498
Improper Validation of	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to	https://w www.qualco	O-QUA-QCS4-181120/499

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
Array Index			<p>improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/500

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
Overflow')			check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	tober-2020-bulletin	
ipq4019_firmware					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ4-181120/501

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
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ4-181120/502

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
			SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ4-181120/503

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	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ4-181120/504
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ4-181120/505
Improper	02-Nov-20	4.6	u'Array index underflow	https://w	O-QUA-IPQ4-

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
Validation of Array Index			<p>issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/506
Buffer Copy without Checking Size of Input ('Classic Buffer	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver</p>	https://www.qualcomm.com/company/product-security/b	O-QUA-IPQ4-181120/507

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
Overflow')			due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	ulletins/oc tober- 2020- bulletin	
ipq8064_firmware					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/508

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
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/509

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
			SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, 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/october-2020-bulletin	O-QUA-IPQ8-181120/510

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
			CVE ID : CVE-2020-11162		
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/511
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/512

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
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/513
Buffer Copy without Checking Size of Input ('Classic	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered</p>	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-181120/514

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
Buffer Overflow')			client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	security/bulletins/october-2020-bulletin	
ipq8074_firmware					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/515

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/516

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
			Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/517

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
			SM8250, SXR2130 CVE ID : CVE-2020-11162		
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/518
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/519

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
			CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ8-181120/520
Buffer Copy without Checking	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query	https://www.qualcomm.com/c	O-QUA-IPQ8-181120/521

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
Size of Input ('Classic Buffer Overflow')			when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	company/product-security/bulletins/october-2020-bulletin	
qca6174a_firmware					
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	O-QUA-QCA6-181120/522

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
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/523

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
			MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/524

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
			MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
qca9377_firmware					
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA9-181120/525

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
			Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA9-181120/526

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
			IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
qca9379_firmware					
Out-of-bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA9-181120/527
sdm429w_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing	https://www.qualco	O-QUA-SDM4-181120/528

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
			downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	mm.com/company/product-security/bulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/529

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	tober-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/530

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
			SXR2130 CVE ID : CVE-2020-3693		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/531
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/532

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/533

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/534
Use After	02-Nov-20	4.4	u'Two threads running	https://w	O-QUA-SDM4-

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
Free			simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/535
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' 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/october-2020-bulletin	O-QUA-SDM4-181120/536

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
			<p>Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>		
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SDM4-181120/537

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
			Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/538

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
			SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
sc7180_firmware					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC71-181120/539
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC71-181120/540

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
			MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC71-181120/541

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
			MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC71-181120/542
Buffer Copy without	02-Nov-20	10	u'Possible buffer overflow while updating output buffer	https://w www.qualco	O-QUA-SC71-181120/543

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
Checking Size of Input ('Classic Buffer Overflow')			for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	mm.com/company/product-security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC71-181120/544

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
			IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
qcm6125_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCM6-181120/545

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
			MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCM6-181120/546
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-QCM6-181120/547

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
			(CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703	2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	O-QUA-QCM6-181120/548

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
			<p>VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	bulletin	
apq8009_firmware					
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without</p>	<p>https://www.qualcomm.com/company/product-security/b</p>	O-QUA-APQ8-181120/549

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
			validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	ulletins/oc tober-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/550

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
			MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/551
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-APQ8-181120/552

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
			InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704	2020-bulletin	
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/oc	O-QUA-APQ8-181120/553

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	tober-2020-bulletin	
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/554

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/555
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/556

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
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/557

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
			SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/558
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/559

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
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/560

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
			IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
apq8098_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/561

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
			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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/562

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
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/563
Improper Restriction of Operations within the Bounds of a Memory	02-Nov-20	4.6	<p>u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/564

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
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	tober-2020-bulletin	
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/565
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in	https://www.qualco	O-QUA-APQ8-181120/566

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
			Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	mm.com/company/product-security/bulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/567

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
			IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/568

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/569
msm8953_firmware					

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 Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/570
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/571

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
			validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	security/bulletins/october-2020-bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/572

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/573

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/574

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
			SDM450, SDM632 CVE ID : CVE-2020-11157		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/575
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/b	O-QUA-MSM8-181120/576

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/577

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/578

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
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/579

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
msm8998_firmware					
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/580
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/581

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
			<p>Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	bulletin	
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/582

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
			Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
nicobar_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/583

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
			MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/584

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/585

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
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3690</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/586
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	<p>u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/587

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
			SXR2130 CVE ID : CVE-2020-3692		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/588
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/589
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This	https://www.qualcomm.com/company/product-security/b	O-QUA-NICO-181120/590

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
			<p>CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	ulletins/oc tober- 2020- bulletin	
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is</p>	https://www.qualcomm.com/company/product-security/bulletins/oc	O-QUA-NICO-181120/591

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
			equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704	tober-2020-bulletin	
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/b	O-QUA-NICO-181120/592

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	ulletins/oc tober- 2020- bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/593

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
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/594

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
			SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/595
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-NICO-181120/596

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	tober-2020-bulletin	
apq8053_firmware					
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon 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/october-2020-bulletin	O-QUA-APQ8-181120/597

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
			Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141		
Out-of-bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/598
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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/october-2020-bulletin	O-QUA-APQ8-181120/599

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
			APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/600
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/601

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
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157		
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/602
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-APQ8-181120/603

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/604

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
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/605

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
			SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/606
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing	https://www.qualco	O-QUA-APQ8-181120/607

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
			downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	mm.com/company/product-security/bulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/608

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	tober-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/609

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
			SXR2130 CVE ID : CVE-2020-3693		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrtr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/610
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/611

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
			<p>sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/612

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
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
mdm9207c_firmware					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/613

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
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/614

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
			MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/615

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
			QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
msm8905_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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/october-2020-bulletin	O-QUA-MSM8-181120/616

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
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/617
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without	https://www.qualcomm.com/company/product-security/b	O-QUA-MSM8-181120/618

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
			validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	ulletins/october-2020-bulletin	
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/619

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
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/620

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
			MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/621

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
			SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/622
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/623

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/624

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
			Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/625

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
			MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
qcn7605_firmware					
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCN7-181120/626
Out-of-bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCN7-181120/627

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
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/product-security/bulletins/october-2020-bulletin	O-QUA-QCN7-181120/628
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/product-security/bulletins/october-2020-bulletin	O-QUA-QCN7-181120/629

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155		
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCN7-181120/630
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-QCN7-181120/631

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
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCN7-181120/632

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
			Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
sdm845_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/633

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
			Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/634

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
			CVE ID : CVE-2020-3673		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/635
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/636

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
			SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/637
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/638

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
			<p>Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	tober-2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to</p>	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-SDM8-181120/639

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
			InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704	2020-bulletin	
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/oc	O-QUA-SDM8-181120/640

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	tober-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/641

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/642

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
			MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/643

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
			SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/644
apq8076_firmware					
Out-of-	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral	https://w www.qualco	O-QUA-APQ8-

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
bounds Read			<p>firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	181120/645
Improper Input	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption	https://www.qualcomm.com/c	O-QUA-APQ8-181120/646

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
Validation			<p>was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632</p> <p>CVE ID : CVE-2020-11157</p>	<p>company/product-security/bulletins/october-2020-bulletin</p>	
ipq5018_firmware					
Improper Input Validation	02-Nov-20	7.8	<p>While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-IPQ5-181120/647

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
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ5-181120/648

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ5-181120/649

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
			QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ5-181120/650
Improper	02-Nov-20	4.6	u'Array index underflow	https://w	O-QUA-IPQ5-

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
Validation of Array Index			<p>issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/651
apq8017_firmware					
Improper Restriction of Operations	02-Nov-20	4.6	<p>u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of</p>	https://www.qualcomm.com/company/p	O-QUA-APQ8-181120/652

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
within the Bounds of a Memory Buffer			qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	product-security/bulletins/october-2020-bulletin	
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/653

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
			CVE ID : CVE-2020-3696		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/654

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/655
Buffer Copy without	02-Nov-20	10	u'Remote code execution can happen by sending a	https://www.qualco	O-QUA-APQ8-181120/656

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
Checking Size of Input ('Classic Buffer Overflow')			carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	mm.com/company/product-security/bulletins/october-2020-bulletin	
apq8096au_firmware					
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/657

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	2020- bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/658

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
			QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/659

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
			CVE ID : CVE-2020-3654		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250</p> <p>CVE ID : CVE-2020-3657</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/660
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message</p>	https://www.qualcomm.com/company/product-security/b	O-QUA-APQ8-181120/661

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
			container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	ulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-APQ8-181120/662

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
			<p>Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>		
Use After Free	02-Nov-20	4.6	<p>u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-APQ8-181120/663

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
			QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
sda845_firmware					
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA8-181120/664
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/b	O-QUA-SDA8-181120/665

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	ulletins/oc tober- 2020- bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA8-181120/666

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA8-181120/667

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
			MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA8-181120/668
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA8-181120/669

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	bulletin	
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA8-181120/670

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
			Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA8-181120/671

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
			QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
sdm636_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/672

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
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/673
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents	https://www.qualcomm.com/company/p	O-QUA-SDM6-181120/674

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
			<p>populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	<p>product-security/bulletins/october-2020-bulletin</p>	
Out-of-bounds Read	02-Nov-20	7.5	<p>u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SDM6-181120/675

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
			2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/676

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
			APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/677

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
			SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/678
Buffer Copy without Checking	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query	https://www.qualcomm.com/c	O-QUA-SDM6-181120/679

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
Size of Input ('Classic Buffer Overflow')			when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	company/product-security/bulletins/october-2020-bulletin	
sdm670_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	O-QUA-SDM6-181120/680

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/681

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
			APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/682
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/683

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
			<p>Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>		
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SDM6-181120/684

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
			SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/685

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/686

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
			SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/687

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
			SXR2130 CVE ID : CVE-2020-11125		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/688
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' 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/october-2020-bulletin	O-QUA-SDM6-181120/689

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
			Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/690

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
			QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
sdm710_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/691

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
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/692
Buffer Copy without	02-Nov-20	4.6	u'A buffer overflow could occur if the API is	https://www.qualco	O-QUA-SDM7-181120/693

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
Checking Size of Input ('Classic Buffer Overflow')			improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	mm.com/company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/694

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
			SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/695
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/696

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
			<p>2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/697

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/698

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
			<p>Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	<p>u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/699

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
			APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/700

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
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/701
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM7-181120/702

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
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	security/bulletins/october-2020-bulletin	
sm6150_firmware					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/703

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
			Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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/october-2020-bulletin	O-QUA-SM61-181120/704

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
			SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/705
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-SM61-181120/706

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	2020- bulletin	
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/707

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
			QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/708
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/709

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
			MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693		
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/710
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/711

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
			<p>Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SM61-181120/712

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
			APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/713

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
			Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/714

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
			SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/715
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/716

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/717

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
			MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM61-181120/718

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3654		
qm215_firmware					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QM21-181120/719

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
Improper Input Validation	02-Nov-20	5	<p>u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632</p> <p>CVE ID : CVE-2020-11157</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QM21-181120/720
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	<p>u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QM21-181120/721

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QM21-181120/722

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
			SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QM21-181120/723

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
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QM21-181120/724
Out-of-bounds Read	02-Nov-20	7.5	<p>u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QM21-181120/725

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
			2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
qcs404_firmware					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/726

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
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/727
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/728

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
			APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/729

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
			SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/730

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
			SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/731

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
			SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/732
Improper	02-Nov-20	4.8	u'Buffer over-read issue in	https://w	O-QUA-QCS4-

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
Input Validation			Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/733
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/734

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
			QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS4-181120/735
Improper	02-Nov-20	4.6	u'Array index underflow	https://w	O-QUA-QCS4-

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
Validation of Array Index			<p>issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/736
sm8150_firmware					
Incorrect Default Permissions	02-Nov-20	4.6	<p>u'An Unaligned address or size can propagate to the database due to improper page permissions and can</p>	https://www.qualcomm.com/company/p	O-QUA-SM81-181120/737

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
			lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	product-security/bulletins/october-2020-bulletin	
Out-of-bounds Read	02-Nov-20	6.4	'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM81-181120/738

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
			Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM81-181120/739

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
			CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM81-181120/740
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto,</p>	https://www.qualcomm.com/company/product-	O-QUA-SM81-181120/741

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM81-181120/742
Improper Restriction of	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check	https://www.qualcomm.com/c	O-QUA-SM81-181120/743

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
Operations within the Bounds of a Memory Buffer			during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM81-181120/744
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM81-181120/745

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
			<p>sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM81-181120/746

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
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM81-181120/747

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM81-181120/748

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM81-181120/749
Use After	02-Nov-20	4.4	u'Two threads running	https://w	O-QUA-SM81-

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
Free			simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/750
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' 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/october-2020-bulletin	O-QUA-SM81-181120/751

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
			<p>Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>		
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SM81-181120/752

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
			Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
mdm9206_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/753

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
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/754

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
			SXR2130 CVE ID : CVE-2020-3684		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrtr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/755
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/756

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
			<p>sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/757

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
mdm9607_firmware					
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/758

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
			MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrtr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/759

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
			CVE ID : CVE-2020-3696		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/760

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
			CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/761

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/762
Buffer Copy without	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of	https://w www.qualco	O-QUA-MDM9-181120/763

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
Checking Size of Input ('Classic Buffer Overflow')			input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	mm.com/company/product-security/bulletins/october-2020-bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/764

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/765

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
			MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/766

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
			SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
mdm9650_firmware					
Out-of- bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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/october-2020-bulletin	O-QUA-MDM9-181120/767

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
			SXR1130 CVE ID : CVE-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/768
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0)	https://www.qualcomm.com/company/p	O-QUA-MDM9-181120/769

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
			<p>from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	product-security/bulletins/october-2020-bulletin	
Out-of-bounds	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check	https://www.qualcomm.com/c	O-QUA-MDM9-181120/770

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
Write			<p>of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>	company/product-security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	5	<p>u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/771

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/772

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
			QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/773

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
			SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
mdm9655_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/774

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
msm8996au_firmware					
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/775
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing</p>	https://www.qualcomm.com/c	O-QUA-MSM8-181120/776

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
			<p>while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>	company/product-security/bulletins/october-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	<p>u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/777

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
			Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/778
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	O-QUA-MSM8-181120/779

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
			<p>VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-</p>	O-QUA-MSM8-181120/780

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/781

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
			APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/782

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
			MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
mdm9625_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/783

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
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
mdm9205_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, 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/october-2020-bulletin	O-QUA-MDM9-181120/784

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
			SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/785
mdm9635m_firmware					
Out-of-	02-Nov-20	6.4	u'Potential out of bounds read while processing	https://w www.qualco	O-QUA-MDM9-

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
bounds Read			downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	mm.com/company/product-security/bulletins/october-2020-bulletin	181120/786
qca9531_firmware					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security	https://www.qualcomm.com/company/product-	O-QUA-QCA9-181120/787

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
			<p>permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24</p> <p>CVE ID : CVE-2020-3696</p>	security/bulletins/october-2020-bulletin	
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA9-181120/788

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
			MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA9-181120/789
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' 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/october-2020-bulletin	O-QUA-QCA9-181120/790

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
			Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
qca9886_firmware					
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA9-181120/791

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
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA9-181120/792

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
			MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157		
qca9980_firmware					
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA9-181120/793
sdm429_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/794

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
			MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/795

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/796

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
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/797

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
			CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	<p>u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632</p> <p>CVE ID : CVE-2020-11157</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/798
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	<p>u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/799

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
			Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/800

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
			SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/801

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
			CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/802
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/803

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	bulletin	
sdm632_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/804

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
			MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/805

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, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/806

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
			QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/807

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
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/808
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/809

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/810

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
			SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/811

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
			SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/812
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/813

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
			check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	tober-2020-bulletin	
msm8917_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/814

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
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/815

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
			MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/816

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
			QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/817

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
			SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/818
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/819

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/820

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
			SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/821
msm8937_firmware					
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and	https://www.qualcomm.com/company/p	O-QUA-MSM8-181120/822

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
			length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703	product-security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection	https://www.qualcomm.com/company/product-	O-QUA-MSM8-181120/823

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
			and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	security/bulletins/october-2020-bulletin	
msm8940_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/824

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
			MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/825

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
			SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/826

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
			SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/827
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/828

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
			APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/829

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3654		
sdm450_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/830

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
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/831
Out-of-bounds Read	02-Nov-20	7.5	<p>u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/832

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
			<p>2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/833

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/834

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
			MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/835
N/A	02-Nov-20	4.6	u'Third-party app may also	https://w	O-QUA-SDM4-

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
			call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/836
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/837

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
			Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
sm8250_firmware					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/838
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/839

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	tober-2020-bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/840

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
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/841

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/842
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/843
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check	https://www.qualcomm.com/c	O-QUA-SM82-181120/844

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
			during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	company/product-security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/845

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
			QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/846

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
			SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/847
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' 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/october-2020-bulletin	O-QUA-SM82-181120/848

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
			Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/849
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in	https://www.qualco	O-QUA-SM82-181120/850

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
			Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	mm.com/company/product-security/bulletins/october-2020-bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/851

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
			Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/852

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
			SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM82-181120/853
Buffer Copy without Checking Size of Input ('Classic	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered	https://www.qualcomm.com/company/product-	O-QUA-SM82-181120/854

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
Buffer Overflow')			<p>client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250</p> <p>CVE ID : CVE-2020-3657</p>	security/bulletins/october-2020-bulletin	
sxr2130_firmware					
Incorrect Default Permissions	02-Nov-20	4.6	<p>u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR2-181120/855

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
			Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR2-181120/856
N/A	02-Nov-20	4.6	u'QSEE reads the access	https://w	O-QUA-SXR2-

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
			<p>permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/857
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-SXR2-181120/858

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR2-181120/859
Improper Restriction of Operations within the Bounds of a	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/b	O-QUA-SXR2-181120/860

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
Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	ulletins/oc tober-2020-bulletin	
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR2-181120/861
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR2-181120/862

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
			<p>Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>		
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SXR2-181120/863

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
			<p>Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	<p>u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR2-181120/864

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
			MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR2-181120/865
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race	https://www.qualcomm.com/c	O-QUA-SXR2-181120/866

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
			condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	company/product-security/bulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR2-181120/867

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
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR2-181120/868

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
			QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
sa6155p_firmware					
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA61-181120/869

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
			CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA61-181120/870
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto,</p>	https://www.qualcomm.com/company/product-	O-QUA-SA61-181120/871

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	security/bulletins/october-2020-bulletin	
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA61-181120/872

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
			Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA61-181120/873
Buffer Copy without Checking Size of Input	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before	https://www.qualcomm.com/company/p	O-QUA-SA61-181120/874

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
('Classic Buffer Overflow')			copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA61-181120/875

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
			QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA61-181120/876
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA61-181120/877

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	tober-2020-bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA61-181120/878

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
			SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA61-181120/879
Improper Validation of	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://www.qualco	O-QUA-SA61-181120/880

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
Array Index			<p>message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
sc8180x_firmware					
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/881

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
			<p>Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>		
Improper Input Validation	02-Nov-20	4.8	<p>u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SC81-181120/882

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
			Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141		
Out-of-bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/883
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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/october-2020-bulletin	O-QUA-SC81-181120/884

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
			APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/885
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' 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/october-2020-bulletin	O-QUA-SC81-181120/886

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
			Snapdragon Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/887
Integer	02-Nov-20	6.4	u'Buffer over-read while	https://w	O-QUA-SC81-

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
Overflow or Wraparound			processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/888
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/889

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
			SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/890

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
			SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/891
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, 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/october-2020-bulletin	O-QUA-SC81-181120/892

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
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/893

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
			Rennell, SA415M, 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-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/894

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
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/896

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
			QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/897

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
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SC81-181120/898

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
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
sdm850_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, 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/october-2020-bulletin	O-QUA-SDM8-181120/899

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
			SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM8-181120/900
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially	https://www.qualcomm.com/c	O-QUA-SDM8-181120/901

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
			<p>compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3690</p>	<p>company/product-security/bulletins/october-2020-bulletin</p>	
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SDM8-181120/902

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
			<p>Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>		
qcm2150_firmware					
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-QCM2-181120/903

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCM2-181120/904

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
			SDM450, SDM632 CVE ID : CVE-2020-11157		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCM2-181120/905
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/b	O-QUA-QCM2-181120/906

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCM2-181120/907

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
			MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCM2-181120/908

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCM2-181120/909
Improper Validation of	02-Nov-20	10	u'Buffer overflow can happen as part of SIP	https://www.qualco	O-QUA-QCM2-181120/910

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
Array Index			<p>message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	<p>u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCM2-181120/911

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
			MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrtr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCM2-181120/912
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-QCM2-181120/913

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
			(CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703	2020-bulletin	
sdx55_firmware					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/oc	O-QUA-SDX5-181120/914

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	tober-2020-bulletin	
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/915

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141		
Out-of- bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/916
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/917

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
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/918
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/919

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/920

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
			SM8250, SXR2130 CVE ID : CVE-2020-11162		
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/921
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/922

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
			IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/923

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
			SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/924
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/925

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/926

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
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/927

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
			SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/928
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-SDX5-181120/929

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX5-181120/930

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
			QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
ar9344_firmware					
Out-of-bounds Read	02-Nov-20	5.8	u'Bluetooth devices does not properly restrict the L2CAP payload length allowing users in radio range to cause a buffer overflow via a crafted Link Layer packet(Equivalent to CVE-2019-17060,CVE-2019-17061 and CVE-2019-17517 in Sweyntooth paper)' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in AR9344 CVE ID : CVE-2020-11114	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-AR93-181120/931
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-AR93-181120/932

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
			<p>2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-AR93-181120/933

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
agatti_firmware					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	O-QUA-AGAT-181120/934

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' 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/october-2020-bulletin	O-QUA-AGAT-181120/935

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
			<p>Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11162</p>		
N/A	02-Nov-20	4.6	<p>u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-AGAT-181120/936

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
			SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-AGAT-181120/937
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	O-QUA-AGAT-181120/938

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	bulletin	
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-AGAT-181120/939

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
			Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-AGAT-181120/940
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper	https://www.qualcomm.com/company/p	O-QUA-AGAT-181120/941

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
			length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	product-security/bulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	O-QUA-AGAT-181120/942

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-AGAT-181120/943
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader	https://www.qualcomm.com/company/product-	O-QUA-AGAT-181120/944

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
			<p>and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-AGAT-181120/945

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
			Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-AGAT-181120/946
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-AGAT-181120/947

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
			<p>in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>		
qrb5165_firmware					
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is</p>	https://www.qualcomm.com/company/product-security/bulletins/oc	O-QUA-QRB5-181120/948

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
			equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704	tober-2020-bulletin	
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/b	O-QUA-QRB5-181120/949

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	ulletins/oc tober- 2020- bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QRB5-181120/950

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
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QRB5-181120/951

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
			IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
qcn7606_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCN7-181120/952
Buffer Copy without Checking Size of Input	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before	https://www.qualcomm.com/company/p	O-QUA-QCN7-181120/953

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
('Classic Buffer Overflow')			copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	product-security/bulletins/october-2020-bulletin	
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCN7-181120/954
sda660_firmware					

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 Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA6-181120/955
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA6-181120/956

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
			validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA6-181120/957

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
			APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA6-181120/958

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
			SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA6-181120/959
Improper Validation of	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://www.qualco	O-QUA-SDA6-181120/960

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
Array Index			<p>message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDA6-181120/961

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
sdm439_firmware					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/962

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
			MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/963

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
			CVE ID : CVE-2020-11157		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/964
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/965

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	tober-2020-bulletin	
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/966

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
			MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/967

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
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM4-181120/968

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
sdm630_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, 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/october-2020-bulletin	O-QUA-SDM6-181120/969

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
			SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/970
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/971

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
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	tober-2020-bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/972

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/973

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
			QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/974

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
			SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/975
Buffer Copy without Checking Size of Input ('Classic Buffer	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver	https://www.qualcomm.com/company/product-security/b	O-QUA-SDM6-181120/976

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
Overflow')			due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	ulletins/oc tober- 2020- bulletin	
sdm660_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/977

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
			Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/978

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
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/979

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
			SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/980

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
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/981

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
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/982

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
			SXR2130 CVE ID : CVE-2020-11125		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/983
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' 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/october-2020-bulletin	O-QUA-SDM6-181120/984

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
			Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/985

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
			SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/986

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDM6-181120/987
mdm9150_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message	https://www.qualcomm.com/company/product-security/b	O-QUA-MDM9-181120/988

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
			container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	ulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/989

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/990

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
			IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/991

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
			MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
mdm9640_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/992

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/993

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
			SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/994
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-MDM9-181120/995

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/996

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
msm8909w_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/997

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
			MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/998

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/999
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, 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/october-2020-bulletin	O-QUA-MSM8-181120/1000

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
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/1001
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-MSM8-181120/1002

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	security/bulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	O-QUA-MSM8-181120/1003

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
			Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MSM8-181120/1004

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
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
qcs605_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1005

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
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1006
Buffer Copy	02-Nov-20	4.6	u'A buffer overflow could	https://w	O-QUA-QCS6-

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
without Checking Size of Input ('Classic Buffer Overflow')			occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/1007
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1008

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
			SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1009
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1010

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
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrtr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1011
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received	https://www.qualcomm.com/company/product-	O-QUA-QCS6-181120/1012

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
			<p>from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into</p>	https://www.qualcomm.com/company/product-security/b	O-QUA-QCS6-181120/1013

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
			<p>dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	ulletins/october-2020-bulletin	
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in</p>	https://www.qualcomm.com/company/product-	O-QUA-QCS6-181120/1014

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
			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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	O-QUA-QCS6-181120/1015

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1016

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
			SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1017

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
			CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1018
sdx20_firmware					
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-SDX2-181120/1019

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	2020- bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1020

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
			<p>Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	<p>u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-3693</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SDX2-181120/1021

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
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1022
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1023

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
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1024

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1025

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
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1026

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
			IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
sm7150_firmware					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM71-181120/1027
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message	https://www.qualcomm.com/company/product-security/b	O-QUA-SM71-181120/1028

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
			container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	ulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM71-181120/1029

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
			Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM71-181120/1030

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
			QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM71-181120/1031
Buffer Copy without Checking Size of Input	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check	https://www.qualcomm.com/company/p	O-QUA-SM71-181120/1032

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
('Classic Buffer Overflow')			of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	product-security/bulletins/october-2020-bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM71-181120/1033

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
			MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM71-181120/1034

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
			Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM71-181120/1035

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
			SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, 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/october-2020-bulletin	O-QUA-SM71-181120/1036

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
			CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	<p>u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11164</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM71-181120/1037
Use After Free	02-Nov-20	4.4	<p>u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM71-181120/1038

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
			APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SM71-181120/1039

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
			SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
sxr1130_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR1-181120/1040

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
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR1-181120/1041
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	<p>u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR1-181120/1042

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
			SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR1-181120/1043
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially	https://www.qualcomm.com/c	O-QUA-SXR1-181120/1044

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
			<p>compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3690</p>	<p>company/product-security/bulletins/october-2020-bulletin</p>	
Out-of-bounds Read	02-Nov-20	7.5	<p>u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SXR1-181120/1045

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
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR1-181120/1046

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
			<p>Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>		
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR1-181120/1047

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
			MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR1-181120/1048

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
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR1-181120/1049
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SXR1-181120/1050

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
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	security/bulletins/october-2020-bulletin	
sdx24_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1051

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
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1052

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
			MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1053
Buffer Copy	02-Nov-20	10	u'Possible buffer overflow	https://w	O-QUA-SDX2-

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
without Checking Size of Input ('Classic Buffer Overflow')			while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/1054
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1055

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
			SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1056

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
			SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1057

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
			SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SDX2-181120/1058
Buffer Copy	02-Nov-20	10	u'Remote code execution can	https://w	O-QUA-SDX2-

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
without Checking Size of Input ('Classic Buffer Overflow')			<p>happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250</p> <p>CVE ID : CVE-2020-3657</p>	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/1059
rennell_firmware					
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-RENN-181120/1060

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	tober-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-RENN-181120/1061

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
			<p>Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11162</p>		
N/A	02-Nov-20	4.6	<p>u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-RENN-181120/1062

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
			SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-RENN-181120/1063
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-RENN-181120/1064

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-RENN-181120/1065

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-RENN-181120/1066
Improper Validation of	02-Nov-20	10	u'Buffer overflow can happen as part of SIP	https://www.qualco	O-QUA-RENN-181120/1067

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
Array Index			<p>message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-RENN-181120/1068

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
			<p>Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>		
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-RENN-181120/1069

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
			SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-RENN-181120/1070
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-RENN-181120/1071

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-RENN-181120/1072

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
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
sa415m_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA41-181120/1073

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
			MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA41-181120/1074

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
			MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA41-181120/1075
Buffer Copy without Checking	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway	https://www.qualcomm.com/c	O-QUA-SA41-181120/1076

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
Size of Input ('Classic Buffer Overflow')			Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	company/product-security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA41-181120/1077

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
			MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA41-181120/1078

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
			QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA41-181120/1079
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-SA41-181120/1080

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA41-181120/1081
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from	https://www.qualcomm.com/company/p	O-QUA-SA41-181120/1082

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
			peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA41-181120/1083

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
			SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA41-181120/1084
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' 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/october-2020-bulletin	O-QUA-SA41-181120/1085

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
			Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
saipan_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SAIP-181120/1086

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
			MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SAIP-181120/1087

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, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-Saip-181120/1088

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
			SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SAIP-181120/1089
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SAIP-181120/1090

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
			Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SAIP-181120/1091
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SAIP-181120/1092
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard	https://www.qualcomm.com/c	O-QUA-SAIP-181120/1093

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
			(interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
Out-of-bounds	02-Nov-20	4.6	u'Out of bound access can happen in MHI command	https://w www.qualco	O-QUA-SAIP-

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
Write			process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	mm.com/company/product-security/bulletins/october-2020-bulletin	181120/1094
Buffer Copy without Checking Size of Input ('Classic Buffer	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SAIP-181120/1095

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
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	tober-2020-bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-Saip-181120/1096

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
			QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SAIP-181120/1097
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id	https://www.qualcomm.com/c	O-QUA-SAIP-181120/1098

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
			before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-Saip-181120/1099

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	2020- bulletin	
ipq6018_firmware					
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ6-181120/1100

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
			IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ6-181120/1101

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
			SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ6-181120/1102
Buffer Copy without	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of	https://www.qualco	O-QUA-IPQ6-181120/1103

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
Checking Size of Input ('Classic Buffer Overflow')			input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	mm.com/company/product-security/bulletins/october-2020-bulletin	
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ6-181120/1104

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
Use After Free	02-Nov-20	4.4	<p>u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11173</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ6-181120/1105
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-IPQ6-181120/1106

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
			Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, 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/october-2020-bulletin	O-QUA-IPQ6-181120/1107

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
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
kamorta_firmware					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1108

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
			QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1109

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
			SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1110
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1111

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
			Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1112

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
			QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1113
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-KAMO-181120/1114

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	2020- bulletin	
Out-of- bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1115

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
			MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1116

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1117
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1118

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
			MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1119
Buffer Copy without	02-Nov-20	10	u'Possible buffer overflow while updating output buffer	https://www.qualco	O-QUA-KAMO-181120/1120

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
Checking Size of Input ('Classic Buffer Overflow')			for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	mm.com/company/product-security/bulletins/october-2020-bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1121

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
			MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-KAMO-181120/1122

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
			MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
bitra_firmware					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1123

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
			QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1124

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
			SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1125
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1126

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
			Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1127

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
			QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1128
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-BITR-181120/1129

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	2020- bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1130

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
			QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1131

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
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1132
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1133

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
			APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693		
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1134
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1135

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
			Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-BITR-181120/1136

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
			Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
qcs610_firmware					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1137

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
			CVE ID : CVE-2020-3638		
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1138
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from	https://www.qualcomm.com/c	O-QUA-QCS6-181120/1139

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
			<p>the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	<p>company/product-security/bulletins/october-2020-bulletin</p>	
N/A	02-Nov-20	7.2	<p>Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-QCS6-181120/1140

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
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1141
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-QCS6-181120/1142

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
			(CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703	2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	O-QUA-QCS6-181120/1143

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
			<p>VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	bulletin	
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-</p>	O-QUA-QCS6-181120/1144

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	2020- bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1145

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
			<p>Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11173</p>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCS6-181120/1146

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
			MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
sa8155p_firmware					
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA81-181120/1147

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
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA81-181120/1148
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA81-181120/1149

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	tober-2020-bulletin	
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA81-181120/1150

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
			QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA81-181120/1151
Buffer Copy without Checking Size of Input ('Classic Buffer	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/b	O-QUA-SA81-181120/1152

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
Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	ulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA81-181120/1153

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
			SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA81-181120/1154
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA81-181120/1155

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA81-181120/1156

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
			CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA81-181120/1157
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack</p>	https://www.qualcomm.com/c	O-QUA-SA81-181120/1158

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
			of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	company/product-security/bulletins/october-2020-bulletin	
sa515m_firmware					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA51-181120/1159

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
			Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA51-181120/1160

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
			SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA51-181120/1161
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA51-181120/1162

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
			<p>Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>		
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA51-181120/1163

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
			<p>Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>		
Improper Input Validation	02-Nov-20	4.8	<p>u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.'</p> <p>in Snapdragon Auto, 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, APQ8053, QCA6390,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SA51-181120/1164

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
			QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA51-181120/1165
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' 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/october-2020-bulletin	O-QUA-SA51-181120/1166

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
			Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155		
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA51-181120/1167
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' 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/october-2020-bulletin	O-QUA-SA51-181120/1168

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
			<p>Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11162</p>		
Integer Overflow or Wraparound	02-Nov-20	6.4	<p>u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55</p> <p>CVE ID : CVE-2020-11169</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-SA51-181120/1169

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
Use After Free	02-Nov-20	4.4	<p>u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11173</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA51-181120/1170
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-SA51-181120/1171

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
			Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
mdm9645_firmware					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-MDM9-181120/1172

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
			MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
qca4531_firmware					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA4-181120/1173

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
			IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
qca6390_firmware					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1174
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1175

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
			<p>Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>		
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	O-QUA-QCA6-181120/1176

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
			QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1177
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0)	https://www.qualcomm.com/company/p	O-QUA-QCA6-181120/1178

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
			<p>from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	product-security/bulletins/october-2020-bulletin	
Out-of-bounds	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check	https://www.qualcomm.com/c	O-QUA-QCA6-181120/1179

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
Write			<p>of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>	company/product-security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	4.8	<p>u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-	O-QUA-QCA6-181120/1180

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	2020-bulletin	
Out-of-bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1181
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1182

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
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1183
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCA6-181120/1184

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
			Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1185

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
			SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1186
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1187

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1188

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
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1189
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	O-QUA-QCA6-181120/1190

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
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	security/bulletins/october-2020-bulletin	
ZTE					
zxa10_eodn_firmware					
Information Exposure	05-Nov-20	4	A ZTE product is impacted by an information leak vulnerability. An attacker could use this vulnerability to obtain the authentication password of the handheld terminal and access the device illegally for operation. This affects: ZXA10 eODN V2.3P2T1 CVE ID : CVE-2020-6877	N/A	O-ZTE-ZXA1-181120/1191
Hardware					

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
imomobile					
verve_connect_vh510					
Use of Hard-coded Credentials	04-Nov-20	5	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 contains undocumented default admin credentials for the web management interface. A remote attacker could exploit this vulnerability to login and execute commands on the device, as well as upgrade the firmware image to a malicious version. CVE ID : CVE-2020-27689	N/A	H-IMO-VERV-181120/1192
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Nov-20	4.9	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 contains a buffer overflow within its web management portal. When a POST request is sent to /boaform/admin/formDOM AINBLK with a large blkDomain value, the Boa server crashes. CVE ID : CVE-2020-27690	N/A	H-IMO-VERV-181120/1193
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-20	4.3	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 allows XSS via URLBlocking Settings, SNMP Settings, and System Log Settings. CVE ID : CVE-2020-27691	N/A	H-IMO-VERV-181120/1194
Cross-Site Request Forgery (CSRF)	04-Nov-20	6.8	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 contains multiple CSRF vulnerabilities	N/A	H-IMO-VERV-181120/1195

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
			<p>within its web management portal. Attackers can, for example, use this to update the TR-069 configuration server settings (responsible for managing devices remotely). This makes it possible to remotely reboot the device or upload malicious firmware.</p> <p>CVE ID : CVE-2020-27692</p>		

Mitsubishielectric

melsec_iq-rj71eip91

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	7.5	<p>Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.</p>	N/A	H-MIT-MELS-181120/1196
--	-----------	-----	---	-----	------------------------

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
			CVE ID : CVE-2020-5653		
Session Fixation	02-Nov-20	5	<p>Session fixation vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5654</p>	N/A	H-MIT-MELS-181120/1197
NULL Pointer Dereference	02-Nov-20	5	<p>NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or</p>	N/A	H-MIT-MELS-181120/1198

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
			<p>before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5655</p>		
N/A	02-Nov-20	7.5	<p>Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network</p>	N/A	H-MIT-MELS-181120/1199

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
			functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5656		
Argument Injection or Modification	02-Nov-20	3.3	Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5657	N/A	H-MIT-MELS-181120/1200
Uncontrolled Resource Consumption	02-Nov-20	5	Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91	N/A	H-MIT-MELS-181120/1201

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
			EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5658		
melsec_iq-rj71pn92					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	7.5	Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface	N/A	H-MIT-MELS-181120/1202

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
			Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5653		
Session Fixation	02-Nov-20	5	Session fixation vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5654	N/A	H-MIT-MELS-181120/1203
NULL	02-Nov-20	5	NULL pointer dereferences	N/A	H-MIT-MELS-

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
Pointer Dereference			vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5655		181120/1204
N/A	02-Nov-20	7.5	Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module	N/A	H-MIT-MELS-181120/1205

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
			First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5656		
Argument Injection or Modification	02-Nov-20	3.3	Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers	N/A	H-MIT-MELS-181120/1206

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
			on adjacent network to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5657		
Uncontrolled Resource Consumption	02-Nov-20	5	Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5658	N/A	H-MIT-MELS-181120/1207
melsec_iq-rd81dl96					
Buffer Copy without Checking Size of Input ('Classic Buffer	02-Nov-20	7.5	Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2	N/A	H-MIT-MELS-181120/1208

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
Overflow')			<p>digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5653</p>		
Session Fixation	02-Nov-20	5	<p>Session fixation vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC</p>	N/A	H-MIT-MELS-181120/1209

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
			UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5654		
NULL Pointer Dereference	02-Nov-20	5	NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5655	N/A	H-MIT-MELS-181120/1210
N/A	02-Nov-20	7.5	Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R	N/A	H-MIT-MELS-181120/1211

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
			<p>series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5656</p>		
Argument Injection or Modification	02-Nov-20	3.3	<p>Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module</p>	N/A	H-MIT-MELS-181120/1212

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
			<p>First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5657</p>		
Uncontrolled Resource Consumption	02-Nov-20	5	<p>Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via</p>	N/A	H-MIT-MELS-181120/1213

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
			a specially crafted packet. CVE ID : CVE-2020-5658		
melsec_iq-rd81mes96n					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	7.5	Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5653	N/A	H-MIT-MELS-181120/1214
Session Fixation	02-Nov-20	5	Session fixation vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller	N/A	H-MIT-MELS-181120/1215

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
			Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5654		
NULL Pointer Dereference	02-Nov-20	5	NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a	N/A	H-MIT-MELS-181120/1216

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
			remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5655		
N/A	02-Nov-20	7.5	Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5656	N/A	H-MIT-MELS-181120/1217
Argument Injection or Modification	02-Nov-20	3.3	Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-	N/A	H-MIT-MELS-181120/1218

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
			<p>R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5657</p>		
Uncontrolled Resource Consumption	02-Nov-20	5	<p>Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before,</p>	N/A	H-MIT-MELS-181120/1219

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
			RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5658		
melsec_iq-rd81opc96					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	7.5	Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	N/A	H-MIT-MELS-181120/1220

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
			CVE ID : CVE-2020-5653		
Session Fixation	02-Nov-20	5	<p>Session fixation vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5654</p>	N/A	H-MIT-MELS-181120/1221
NULL Pointer Dereference	02-Nov-20	5	<p>NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or</p>	N/A	H-MIT-MELS-181120/1222

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
			<p>before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.</p> <p>CVE ID : CVE-2020-5655</p>		
N/A	02-Nov-20	7.5	<p>Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network</p>	N/A	H-MIT-MELS-181120/1223

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
			functions of the products or execute a malicious program via a specially crafted packet. CVE ID : CVE-2020-5656		
Argument Injection or Modification	02-Nov-20	3.3	Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5657	N/A	H-MIT-MELS-181120/1224
Uncontrolled Resource Consumption	02-Nov-20	5	Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91	N/A	H-MIT-MELS-181120/1225

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
			EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet. CVE ID : CVE-2020-5658		
Moxa					
vport_461					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Nov-20	10	A command injection vulnerability exists in Moxa Inc VPort 461 Series Firmware Version 3.4 or lower that could allow a remote attacker to execute arbitrary commands in Moxa's VPort 461 Series Industrial Video Servers. CVE ID : CVE-2020-23639	N/A	H-MOX-VPOR-181120/1226
Qualcomm					
mdm9206					
Out-of-	02-Nov-20	6.4	u'Potential out of bounds read while processing	https://www.qualco	H-QUA-MDM9-

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
bounds Read			downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	mm.com/company/product-security/bulletins/october-2020-bulletin	181120/1227
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1228

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
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	tober-2020-bulletin	
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, 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/october-2020-bulletin	H-QUA-MDM9-181120/1229

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
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1230

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
			QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1231

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
			SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
mdm9607					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1232

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1233
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-MDM9-181120/1234

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1235

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
			MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1236

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
			QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1237

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
			CVE ID : CVE-2020-3684		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1238
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1239

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
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1240

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
msm8909w					
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1241

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
			Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1242

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
			SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1243
Buffer Copy without	02-Nov-20	10	u'Remote code execution can happen by sending a	https://www.qualco	H-QUA-MSM8-181120/1244

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
Checking Size of Input ('Classic Buffer Overflow')			carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	mm.com/company/product-security/bulletins/october-2020-bulletin	
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-MSM8-181120/1245

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
			Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1246

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
			Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1247
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular	https://www.qualcomm.com/company/product-security/b	H-QUA-MSM8-181120/1248

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
			process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	ulletins/oc tober- 2020- bulletin	
msm8996au					
Out-of- bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1249

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
			MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1250

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1251
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, 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/october-2020-bulletin	H-QUA-MSM8-181120/1252

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
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1253

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
			QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1254

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
			SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1255
Buffer Copy without Checking	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query	https://www.qualcomm.com/c	H-QUA-MSM8-181120/1256

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
Size of Input ('Classic Buffer Overflow')			when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	company/product-security/bulletins/october-2020-bulletin	
qca6574au					
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-QCA6-181120/1257

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	bulletin	
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, 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/october-2020-bulletin	H-QUA-QCA6-181120/1258

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
			MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1259

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
			SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1260
Buffer Copy without Checking	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query	https://www.qualcomm.com/c	H-QUA-QCA6-181120/1261

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
Size of Input ('Classic Buffer Overflow')			when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	company/product-security/bulletins/october-2020-bulletin	
qcs405					
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-QCS4-181120/1262

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1263

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
			<p>Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-QCS4-181120/1264

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
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1265

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
			APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1266

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
			QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1267

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
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1268
Buffer Copy without Checking Size of Input ('Classic	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1269

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
Buffer Overflow')			client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	security/bulletins/october-2020-bulletin	
qcs605					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1270

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
			<p>Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>		
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-QCS6-181120/1271

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
			MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1272
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1273

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
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1274

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
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1275
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, 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/october-2020-bulletin	H-QUA-QCS6-181120/1276

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
			APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1277

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
			QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1278

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
			QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1279

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
			SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1280
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause	https://www.qualcomm.com/c	H-QUA-QCS6-181120/1281

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
			<p>privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11164</p>	<p>company/product-security/bulletins/october-2020-bulletin</p>	
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-QCS6-181120/1282

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
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1283

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
			SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
sda660					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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/october-2020-bulletin	H-QUA-SDA6-181120/1284

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
			SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDA6-181120/1285
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SDA6-181120/1286

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	2020-bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDA6-181120/1287

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
			QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDA6-181120/1288

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
			SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDA6-181120/1289
Buffer Copy without Checking Size of Input ('Classic Buffer	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver	https://www.qualcomm.com/company/product-security/b	H-QUA-SDA6-181120/1290

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
Overflow')			due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	ulletins/oc tober- 2020- bulletin	
sdm439					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1291

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
			Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1292

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
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1293

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
			MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1294

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
			SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1295
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1296

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1297

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
			Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
sdm630					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1298

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
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1299
N/A	02-Nov-20	4.6	u'QSEE reads the access	https://w	H-QUA-SDM6-

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
			<p>permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/1300
Out-of-bounds Read	02-Nov-20	7.5	<p>u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue</p>	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SDM6-181120/1301

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
			(CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703	2020-bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-SDM6-181120/1302

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
			Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1303

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
			SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1304

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1305
sdm660					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message	https://www.qualcomm.com/company/product-security/b	H-QUA-SDM6-181120/1306

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
			container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	ulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1307

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
			<p>Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>		
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SDM6-181120/1308

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
			QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1309

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
			QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1310

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
			QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1311

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
			SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1312
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1313

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1314

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
			MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1315

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
			SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1316
sdx20					
Out-of-	02-Nov-20	6.4	u'Potential out of bounds read while processing	https://w www.qualco	H-QUA-SDX2-

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
bounds Read			downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	mm.com/company/product-security/bulletins/october-2020-bulletin	181120/1317
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX2-181120/1318

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
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	tober-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX2-181120/1319

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
			Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX2-181120/1320
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-SDX2-181120/1321

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
			2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703	bulletin	
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-SDX2-181120/1322

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
			<p>in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-SDX2-181120/1323

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' 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/october-2020-bulletin	H-QUA-SDX2-181120/1324

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
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
mdm9150					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1325

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
			MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1326

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
			SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1327

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
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1328
mdm9640					
Out-of-	02-Nov-20	6.4	u'Potential out of bounds read while processing	https://w www.qualco	H-QUA-MDM9-

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
bounds Read			downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	mm.com/company/product-security/bulletins/october-2020-bulletin	181120/1329
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1330

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
			equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704	tober-2020-bulletin	
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in	https://www.qualcomm.com/company/product-security/b	H-QUA-MDM9-181120/1331

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
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1332

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
			MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1333

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
			SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
mdm9650					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1334

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
			SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1335
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' 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/october-2020-bulletin	H-QUA-MDM9-181120/1336

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
			Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, 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/october-2020-bulletin	H-QUA-MDM9-181120/1337

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
			IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1338

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
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1339

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
			SXR2130 CVE ID : CVE-2020-3684		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1340

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
			SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
sdX24					
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX2-181120/1341

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX2-181120/1342
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SDX2-181120/1343

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	2020- bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX2-181120/1344

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
			<p>Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>		
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SDX2-181120/1345

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
			SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX2-181120/1346
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX2-181120/1347

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
			IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX2-181120/1348

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
			SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX2-181120/1349

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
			SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
ipq4019					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ4-181120/1350
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in	https://www.qualcomm.com/company/product-	H-QUA-IPQ4-181120/1351

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
			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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-IPQ4-181120/1352

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	bulletin	
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ4-181120/1353
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-IPQ4-181120/1354

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ4-181120/1355

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
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ4-181120/1356

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
			MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
ipq8064					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ8-181120/1357
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-181120/1358

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
			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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-IPQ8-181120/1359

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	bulletin	
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ8-181120/1360
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-IPQ8-181120/1361

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ8-181120/1362

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
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ8-181120/1363

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
			MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
ipq8074					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ8-181120/1364
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ8-181120/1365

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
			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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-IPQ8-181120/1366

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	bulletin	
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ8-181120/1367
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ8-181120/1368

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ8-181120/1369

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
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ8-181120/1370

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
			MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
qca6174a					
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1371

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
			QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1372

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
			QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1373
qca9377					
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received	https://www.qualcomm.com/company/product-	H-QUA-QCA9-181120/1374

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
			<p>from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into</p>	https://www.qualcomm.com/company/product-security/b	H-QUA-QCA9-181120/1375

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
			<p>dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	ulletins/october-2020-bulletin	
qca9379					
Out-of-bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to	https://www.qualcomm.com/c	H-QUA-QCA9-181120/1376

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
			lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	company/product-security/bulletins/october-2020-bulletin	
sdm429w					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1377

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
			QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1378

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1379
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1380

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
			MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1381

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
			SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1382
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/b	H-QUA-SDM4-181120/1383

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	ulletins/oc tober- 2020- bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1384

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
			SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1385

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
			SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1386
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SDM4-181120/1387

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
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	2020- bulletin	
sc7180					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC71-181120/1388

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
			Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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/october-2020-bulletin	H-QUA-SC71-181120/1389

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
			SXR1130 CVE ID : CVE-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC71-181120/1390
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor'	https://www.qualcomm.com/company/p	H-QUA-SC71-181120/1391

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
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC71-181120/1392
Improper Input	02-Nov-20	7.8	u'While processing invalid connection request PDU	https://www.qualco	H-QUA-SC71-181120/1393

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
Validation			<p>which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	

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
qcm6125					
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM6-181120/1394
Buffer Copy without Checking	02-Nov-20	10	<p>u'Possible buffer overflow while updating output buffer for IMEI and Gateway</p>	https://www.qualcomm.com/c	H-QUA-QCM6-181120/1395

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
Size of Input ('Classic Buffer Overflow')			Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	company/product-security/bulletins/october-2020-bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM6-181120/1396

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
			MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM6-181120/1397

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
			MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
apq8009					
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1398

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
			SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1399
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1400

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1401

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
			MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1402

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
			QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1403
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-APQ8-181120/1404

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1405
Buffer Copy without Checking Size of Input	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from	https://www.qualcomm.com/company/p	H-QUA-APQ8-181120/1406

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
('Classic Buffer Overflow')			MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	product-security/bulletins/october-2020-bulletin	
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' 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/october-2020-bulletin	H-QUA-APQ8-181120/1407

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
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1408

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
			SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1409
apq8098					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport	https://www.qualcomm.com/c	H-QUA-APQ8-181120/1410

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
			<p>message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	<p>company/product-security/bulletins/october-2020-bulletin</p>	
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-</p>	H-QUA-APQ8-181120/1411

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	2020- bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1412

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
			MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1413
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular	https://www.qualcomm.com/company/product-security/b	H-QUA-APQ8-181120/1414

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
			process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	ulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1415

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
			SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1416
Improper	02-Nov-20	10	u'Buffer overflow occurs	https://w	H-QUA-APQ8-

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
Validation of Array Index			<p>while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/1417
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1418

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
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
msm8953					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1419

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
			MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1420

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
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1421

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1422

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
			SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1423
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' 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/october-2020-bulletin	H-QUA-MSM8-181120/1424

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
			<p>Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11162</p>		
Use After Free	02-Nov-20	4.4	<p>u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-MSM8-181120/1425

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
			SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1426

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
			SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1427
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-MSM8-181120/1428

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
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	2020- bulletin	
msm8998					
Out-of- bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1429

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
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1430

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
			MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1431

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
			SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
nicobar					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-NICO-181120/1432

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
			CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-NICO-181120/1433
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-NICO-181120/1434

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	tober-2020-bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-NICO-181120/1435

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
			SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-NICO-181120/1436
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information	https://www.qualcomm.com/company/product-	H-QUA-NICO-181120/1437

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
			Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	security/bulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-NICO-181120/1438

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-NICO-181120/1439

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
			MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-NICO-181120/1440
Buffer Copy without Checking	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway	https://www.qualcomm.com/c	H-QUA-NICO-181120/1441

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
Size of Input ('Classic Buffer Overflow')			Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	company/product-security/bulletins/october-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-NICO-181120/1442
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/b	H-QUA-NICO-181120/1443

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
			Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	ulletins/oc tober-2020-bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/oc tober-2020-bulletin	H-QUA-NICO-181120/1444

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
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-NICO-181120/1445

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
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
apq8053					
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1446
Out-of-bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1447

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
			Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1448
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1449

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1450
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/b	H-QUA-APQ8-181120/1451

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
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	ulletins/oc tober- 2020- bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1452

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
			SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1453
Improper	02-Nov-20	10	u'Buffer overflow occurs	https://w	H-QUA-APQ8-

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
Validation of Array Index			<p>while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/1454
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1455

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
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1456

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
			MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1457

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
			SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1458
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, 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/october-2020-bulletin	H-QUA-APQ8-181120/1459

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
			APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1460

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
			QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1461

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
			QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
mdm9207c					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1462
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of	https://www.qualcomm.com/c	H-QUA-MDM9-181120/1463

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
			check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703	company/product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is	https://www.qualcomm.com/company/p	H-QUA-MDM9-181120/1464

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
('Classic Buffer Overflow')			<p>accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250</p> <p>CVE ID : CVE-2020-3657</p>	product-security/bulletins/october-2020-bulletin	
msm8905					
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1465

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
			Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1466

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
			Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1467

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
			SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1468
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This	https://www.qualcomm.com/company/product-security/b	H-QUA-MSM8-181120/1469

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
			<p>CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	ulletins/oc tober- 2020- bulletin	
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute,</p>	https://www.qualcomm.com/company/product-security/bulletins/oc	H-QUA-MSM8-181120/1470

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	tober-2020-bulletin	
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1471

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1472

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
			SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1473
Buffer Copy without Checking	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query	https://www.qualcomm.com/c	H-QUA-MSM8-181120/1474

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
Size of Input ('Classic Buffer Overflow')			when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	company/product-security/bulletins/october-2020-bulletin	
qcn7605					
Improper Input Validation	02-Nov-20	7.8	While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-QCN7-181120/1475

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
			<p>VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	bulletin	
Improper Input Validation	02-Nov-20	4.8	<p>u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.'</p> <p>in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-QCN7-181120/1476

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	2020-bulletin	
Out-of-bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCN7-181120/1477
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCN7-181120/1478

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
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCN7-181120/1479
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon	https://www.qualcomm.com/company/p	H-QUA-QCN7-181120/1480

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
			Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	security/bulletins/october-2020-bulletin	
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCN7-181120/1481
sdm845					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport	https://www.qualcomm.com/c	H-QUA-SDM8-181120/1482

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
			<p>message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	<p>company/product-security/bulletins/october-2020-bulletin</p>	
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-</p>	H-QUA-SDM8-181120/1483

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM8-181120/1484
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents	https://www.qualcomm.com/company/p	H-QUA-SDM8-181120/1485

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
			<p>populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	<p>product-security/bulletins/october-2020-bulletin</p>	
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SDM8-181120/1486

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
			Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM8-181120/1487

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
			MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM8-181120/1488

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
			QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM8-181120/1489

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
			SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM8-181120/1490

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
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM8-181120/1491
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM8-181120/1492

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
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, 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/october-2020-bulletin	H-QUA-SDM8-181120/1493

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
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
apq8076					
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1494

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
			<p>Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	5	<p>u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-APQ8-181120/1495

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
			SDM450, SDM632 CVE ID : CVE-2020-11157		
ipq5018					
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/products-security/bulletins/october-2020-bulletin	H-QUA-IPQ5-181120/1496

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
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ5-181120/1497

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
			CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ5-181120/1498
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ5-181120/1499

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	tober-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ5-181120/1500

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
			IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
apq8017					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1501
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted	https://www.qualcomm.com/c	H-QUA-APQ8-181120/1502

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
			and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	company/product-security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1503

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
			<p>Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>		
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-APQ8-181120/1504

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
			APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1505

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
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
apq8096au					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1506

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
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1507
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule	https://www.qualco	H-QUA-APQ8-181120/1508

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
			in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	mm.com/company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1509

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
			SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1510

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
			SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-APQ8-181120/1511
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-APQ8-181120/1512

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
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	2020- bulletin	
sda845					
Out-of- bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDA8-181120/1513

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
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDA8-181120/1514
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents	https://www.qualcomm.com/company/p	H-QUA-SDA8-181120/1515

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
			<p>populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	<p>product-security/bulletins/october-2020-bulletin</p>	
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SDA8-181120/1516

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
			Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDA8-181120/1517

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
			Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/product-security/bulletins/october-2020-bulletin	H-QUA-SDA8-181120/1518

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
			SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDA8-181120/1519
Buffer Copy without	02-Nov-20	10	u'Remote code execution can happen by sending a	https://w www.qualco	H-QUA-SDA8-181120/1520

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
Checking Size of Input ('Classic Buffer Overflow')			carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	mm.com/company/product-security/bulletins/october-2020-bulletin	
sdm636					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SDM6-181120/1521

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1522

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
			Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1523

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
			SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1524

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
			QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1525
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1526

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	tober-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1527

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
			Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1528

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
			MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
sdm670					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1529

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1530
Buffer Copy without Checking	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE	https://www.qualcomm.com/c	H-QUA-SDM6-181120/1531

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
Size of Input ('Classic Buffer Overflow')			init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1532

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
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1533
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1534

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
			<p>sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1535

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
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1536

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1537

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
			SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1538

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
			SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1539
sdm710					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM7-181120/1540

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
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	tober-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM7-181120/1541

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
			<p>Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	<p>u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130</p> <p>CVE ID : CVE-2020-3678</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM7-181120/1542
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SDM7-181120/1543

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	2020-bulletin	
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM7-181120/1544

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
			QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM7-181120/1545

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
			QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM7-181120/1546

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
			QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM7-181120/1547

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
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM7-181120/1548
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue	https://www.qualcomm.com/company/p	H-QUA-SDM7-181120/1549

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
			<p>due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11164</p>	<p>product-security/bulletins/october-2020-bulletin</p>	
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SDM7-181120/1550

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
			MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM7-181120/1551

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
			SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
qcs404					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1552
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1553

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
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1554
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1555

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	tober-2020-bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1556

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
			Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1557

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
			IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1558

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
			QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1559
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-QCS4-181120/1560

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	2020- bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1561

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
			IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS4-181120/1562

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
			SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
sxr1130					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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/october-2020-bulletin	H-QUA-SXR1-181120/1563

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
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR1-181120/1564
Buffer Copy without Checking Size of Input ('Classic Buffer	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/b	H-QUA-SXR1-181120/1565

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
Overflow')			Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	ulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR1-181120/1566

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
			SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR1-181120/1567
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR1-181120/1568

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR1-181120/1569

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
			<p>Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>		
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SXR1-181120/1570

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
			<p>Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>		
N/A	02-Nov-20	4.6	<p>u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SXR1-181120/1571

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
			SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR1-181120/1572

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
			CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR1-181120/1573
sm6150					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SM61-181120/1574

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	2020-bulletin	
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1575

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1576
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from	https://www.qualcomm.com/c	H-QUA-SM61-181120/1577

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
			<p>the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	7.2	<p>Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1578

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
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1579
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SM61-181120/1580

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	2020-bulletin	
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1581
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1582

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
			<p>Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SM61-181120/1583

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
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1584

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1585

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
			QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1586
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/b	H-QUA-SM61-181120/1587

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1588

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM61-181120/1589

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
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
sm8150					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1590
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1591

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
			Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1592

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
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1593

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
			SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1594
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1595

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
			Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1596
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1597

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 Read	02-Nov-20	7.5	<p>u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1598

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
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1599

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
			CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1600
Buffer Copy without Checking	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation	https://www.qualcomm.com/c	H-QUA-SM81-181120/1601

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
Size of Input ('Classic Buffer Overflow')			<p>of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11162</p>	company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	<p>u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1602

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
			APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1603

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
			CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM81-181120/1604
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack</p>	https://www.qualcomm.com/c	H-QUA-SM81-181120/1605

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
			of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	company/product-security/bulletins/october-2020-bulletin	
mdm9625					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1606

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
			Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
mdm9205					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1607

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
			MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1608

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
			MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
mdm9655					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1609

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
			Rennell, SA415M, 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-2020-3670		
mdm9635m					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MDM9-181120/1610

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
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
qca9531					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA9-181120/1611
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in	https://www.qualcomm.com/company/product-	H-QUA-QCA9-181120/1612

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
			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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	security/bulletins/october-2020-bulletin	
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-QCA9-181120/1613

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
			CVE ID : CVE-2020-11172	bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA9-181120/1614
qca9886					
Improper Input	02-Nov-20	7.8	u'While processing invalid connection request PDU	https://w www.qualco	H-QUA-QCA9-181120/1615

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
Validation			<p>which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	

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
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA9-181120/1616
qca9980					
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA9-181120/1617
qm215					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport	https://www.qualcomm.com/c	H-QUA-QM21-181120/1618

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
			<p>message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	<p>company/product-security/bulletins/october-2020-bulletin</p>	
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-</p>	H-QUA-QM21-181120/1619

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	2020-bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QM21-181120/1620

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
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QM21-181120/1621

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
			MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QM21-181120/1622

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QM21-181120/1623
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-QM21-181120/1624

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	bulletin	
sm7150					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71-181120/1625

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
			SM8250, SXR2130 CVE ID : CVE-2020-3638		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71-181120/1626
Improper Validation of	02-Nov-20	10	u'Buffer overflow can happen as part of SIP	https://www.qualco	H-QUA-SM71-181120/1627

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
Array Index			<p>message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3673</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71-181120/1628

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
			<p>Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>		
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SM71-181120/1629

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
			SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71-181120/1630
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71-181120/1631

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71-181120/1632

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
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71-181120/1633

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
			IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71-181120/1634

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
			QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71-181120/1635
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71-181120/1636

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	tober- 2020- bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM71- 181120/1637

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
			QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
sdm429					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1638

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
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1639
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral	https://www.qualco	H-QUA-SDM4-181120/1640

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
			<p>firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
Out-of-bounds	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check</p>	https://www.qualcomm.com/c	H-QUA-SDM4-181120/1641

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
Write			<p>of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>	company/product-security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	5	<p>u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1642

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1643

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
			SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1644
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'	https://www.qualcomm.com/company/p	H-QUA-SDM4-181120/1645

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
			in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	product- security/b ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-SDM4-181120/1646

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1647

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
			IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
sdm632					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1648

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
			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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1649

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 Read	02-Nov-20	7.5	<p>u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1650

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	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1651
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection	https://www.qualcomm.com/company/product-	H-QUA-SDM6-181120/1652

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
			and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1653

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
			QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM6-181120/1654
Improper	02-Nov-20	4.6	u'Array index underflow	https://w	H-QUA-SDM6-

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
Validation of Array Index			<p>issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/1655
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto,</p>	https://www.qualcomm.com/company/product-security/b	H-QUA-SDM6-181120/1656

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	ulletins/oc tober- 2020- bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, 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/october-2020-bulletin	H-QUA-SDM6-181120/1657

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
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
msm8917					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1658

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, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1659

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1660

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
			SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1661
Improper Input	02-Nov-20	5	u'Lack of handling unexpected control	https://www.qualco	H-QUA-MSM8-181120/1662

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
Validation			<p>messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632</p> <p>CVE ID : CVE-2020-11157</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	<p>u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1663

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
			MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1664
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack	https://www.qualcomm.com/c	H-QUA-MSM8-181120/1665

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
			of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	company/product-security/bulletins/october-2020-bulletin	
msm8937					
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1666

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
			<p>sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	5	<p>u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1667

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
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157		
msm8940					
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1668
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in PerfDump and cause privilege escalation issue	https://www.qualcomm.com/company/p	H-QUA-MSM8-181120/1669

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
			<p>due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11164</p>	<p>product-security/bulletins/october-2020-bulletin</p>	
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-MSM8-181120/1670

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
			SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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/october-2020-bulletin	H-QUA-MSM8-181120/1671

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
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-MSM8-181120/1672
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This	https://www.qualcomm.com/company/product-security/b	H-QUA-MSM8-181120/1673

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
			<p>CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in 'sweyntooth paper' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	<p>ulletins/october-2020-bulletin</p>	
sdm450					
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information</p>	<p>https://www.qualcomm.com/company/product-</p>	H-QUA-SDM4-181120/1674

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
			<p>Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	security/bulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-SDM4-181120/1675

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1676

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
			Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1677

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
			Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1678
Buffer Copy without	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of	https://w www.qualco	H-QUA-SDM4-181120/1679

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
Checking Size of Input ('Classic Buffer Overflow')			input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	mm.com/company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1680

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
			Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM4-181120/1681

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3654		
sm8250					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1682
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1683

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
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1684

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
			SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1685
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1686

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
			Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1687
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1688

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
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1689

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
			CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1690
Improper Input Validation	02-Nov-20	4.8	<p>u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of</p>	https://www.qualcomm.com/c	H-QUA-SM82-181120/1691

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
			L2cap configuration request received from peer device.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	company/product-security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1692
Buffer Copy without	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of	https://www.qualco	H-QUA-SM82-181120/1693

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
Checking Size of Input ('Classic Buffer Overflow')			input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	mm.com/company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1694

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
			Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1695

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
			SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1696
Improper Validation of	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://www.qualco	H-QUA-SM82-181120/1697

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
Array Index			<p>message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	<p>u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SM82-181120/1698

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
sxr2130					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1699

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
			MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1700

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
			SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1701
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SXR2-181120/1702

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1703

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
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1704
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation	https://www.qualcomm.com/company/p	H-QUA-SXR2-181120/1705

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
			before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	roduct- security/b ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1706

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
			Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1707

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
			SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1708
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SXR2-181120/1709

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1710
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1711

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
			CVE ID : CVE-2020-3694		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SXR2-181120/1712

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3704		
sa6155p					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA61-181120/1713

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA61-181120/1714
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA61-181120/1715

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
			SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA61-181120/1716
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access	https://www.qualcomm.com/company/product-	H-QUA-SA61-181120/1717

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
			control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	security/bulletins/october-2020-bulletin	
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA61-181120/1718

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
Use After Free	02-Nov-20	4.4	<p>u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11173</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA61-181120/1719
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA61-181120/1720

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
			Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA61-181120/1721

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
			MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/products-security/bulletins/october-2020-bulletin	H-QUA-SA61-181120/1722

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA61-181120/1723
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor'	https://www.qualcomm.com/company/p	H-QUA-SA61-181120/1724

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
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	product-security/bulletins/october-2020-bulletin	
sc8180x					
Incorrect Default Permissions	02-Nov-20	4.6	'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1725

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
			CVE ID : CVE-2020-3638		
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1726
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from	https://www.qualcomm.com/c	H-QUA-SC81-181120/1727

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
			<p>the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	<p>company/product-security/bulletins/october-2020-bulletin</p>	
N/A	02-Nov-20	7.2	<p>Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SC81-181120/1728

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
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1729
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SC81-181120/1730

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
			(CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703	2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-SC81-181120/1731

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
			<p>VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	bulletin	
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SC81-181120/1732

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	2020- bulletin	
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1733

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
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141		
Out-of-bounds Write	02-Nov-20	10	'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1734
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' 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/october-2020-bulletin	H-QUA-SC81-181120/1735

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
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1736
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1737

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1738

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
			SM8250, SXR2130 CVE ID : CVE-2020-11162		
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1739
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1740

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
			IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1741

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
			SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SC81-181120/1742

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
sdm850					
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM8-181120/1743
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from</p>	https://www.qualcomm.com/c	H-QUA-SDM8-181120/1744

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
			<p>the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	<p>company/product-security/bulletins/october-2020-bulletin</p>	
N/A	02-Nov-20	7.2	<p>Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SDM8-181120/1745

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
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	bulletin	
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDM8-181120/1746

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
			MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
qcm2150					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM2-181120/1747

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
			QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM2-181120/1748

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM2-181120/1749
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM2-181120/1750

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
			MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM2-181120/1751

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
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM2-181120/1752

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
			SXR2130 CVE ID : CVE-2020-11125		
Improper Input Validation	02-Nov-20	5	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM2-181120/1753
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' 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/october-2020-bulletin	H-QUA-QCM2-181120/1754

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
			<p>Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11162</p>		
N/A	02-Nov-20	4.6	<p>u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-QCM2-181120/1755

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
			SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCM2-181120/1756
Improper Validation of	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://www.qualco	H-QUA-QCM2-181120/1757

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
Array Index			<p>message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
sdx55					
Incorrect Default Permissions	02-Nov-20	4.6	<p>u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1758

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
			Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638		
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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/october-2020-bulletin	H-QUA-SDX5-181120/1759

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
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1760
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem	https://www.qualco	H-QUA-SDX5-181120/1761

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
			crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	mm.com/company/product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1762

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
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1763

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
			CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1764
Improper Input Validation	02-Nov-20	4.8	<p>u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of</p>	https://www.qualcomm.com/c	H-QUA-SDX5-181120/1765

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
			L2cap configuration request received from peer device.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	company/product-security/bulletins/october-2020-bulletin	
Out-of-bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1766
Buffer Copy without Checking Size of Input	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size	https://www.qualcomm.com/company/p	H-QUA-SDX5-181120/1767

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
('Classic Buffer Overflow')			before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1768

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
Improper Input Validation	02-Nov-20	4.8	<p>u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250</p> <p>CVE ID : CVE-2020-11156</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1769
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	<p>u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1770

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
			QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1771
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SDX5-181120/1772

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1773

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
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SDX5-181120/1774

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
			MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
ar9344					
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AR93-181120/1775

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
			QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AR93-181120/1776

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
			QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Read	02-Nov-20	5.8	u'Bluetooth devices does not properly restrict the L2CAP payload length allowing users in radio range to cause a buffer overflow via a crafted Link Layer packet(Equivalent to CVE-2019-17060,CVE-2019-17061 and CVE-2019-17517 in Sweyntooth paper)' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in AR9344 CVE ID : CVE-2020-11114	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AR93-181120/1777
agatti					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AGAT-181120/1778

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
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AGAT-181120/1779

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AGAT-181120/1780
Use After	02-Nov-20	4.4	u'Two threads running	https://w	H-QUA-AGAT-

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
Free			simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/1781
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' 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/october-2020-bulletin	H-QUA-AGAT-181120/1782

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
			<p>Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>		
Incorrect Default Permissions	02-Nov-20	4.6	<p>u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-AGAT-181120/1783

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
			SM8250, SXR2130 CVE ID : CVE-2020-3638		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AGAT-181120/1784
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-AGAT-181120/1785

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AGAT-181120/1786

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
			Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AGAT-181120/1787
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AGAT-181120/1788

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	bulletin	
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AGAT-181120/1789

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
			Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AGAT-181120/1790
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-AGAT-181120/1791

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
qrb5165					
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QRB5-181120/1792

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
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-QRB5-181120/1793

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
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' 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/october-2020-bulletin	H-QUA-QRB5-181120/1794

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
			Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QRB5-181120/1795

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
			MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
qcn7606					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCN7-181120/1796
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-QCN7-181120/1797

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
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	2020-bulletin	
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCN7-181120/1798
rennell					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can	https://www.qualcomm.com/company/p	H-QUA-RENN-181120/1799

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
			lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	product-security/bulletins/october-2020-bulletin	
Out-of-bounds Read	02-Nov-20	6.4	'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-RENN-181120/1800

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
			Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-RENN-181120/1801

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
			CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3684</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-RENN-181120/1802
N/A	02-Nov-20	7.2	<p>u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto,</p>	https://www.qualcomm.com/company/product-	H-QUA-RENN-181120/1803

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-RENN-181120/1804
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of	https://www.qualcomm.com/c	H-QUA-RENN-181120/1805

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
			<p>check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>	company/product-security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0)</p>	https://www.qualcomm.com/company/p	H-QUA-RENN-181120/1806

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
			<p>from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>	product-security/bulletins/october-2020-bulletin	
Out-of-bounds	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check	https://www.qualcomm.com/c	H-QUA-RENN-181120/1807

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
Write			<p>of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>	company/product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	<p>u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-RENN-181120/1808

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	2020- bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-RENN-181120/1809

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
			SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-RENN-181120/1810
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation	https://www.qualcomm.com/company/p	H-QUA-RENN-181120/1811

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
			before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	roduct- security/b ulletins/oc tober- 2020- bulletin	
sa415m					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' 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/october-2020-bulletin	H-QUA-SA41-181120/1812

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
			<p>Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>		
Improper Input Validation	02-Nov-20	4.8	<p>u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.'</p> <p>in Snapdragon Auto, 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, APQ8053, QCA6390,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SA41-181120/1813

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
			QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA41-181120/1814
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' 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/october-2020-bulletin	H-QUA-SA41-181120/1815

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
			Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155		
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA41-181120/1816
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' 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/october-2020-bulletin	H-QUA-SA41-181120/1817

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
			<p>Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2020-11162</p>		
Integer Overflow or Wraparound	02-Nov-20	6.4	<p>u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55</p> <p>CVE ID : CVE-2020-11169</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SA41-181120/1818

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
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA41-181120/1819
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA41-181120/1820

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
			<p>Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3670</p>	security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	<p>u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-SA41-181120/1821

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	bulletin	
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA41-181120/1822

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
			SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA41-181120/1823
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA41-181120/1824

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
			<p>Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3704</p>		
saipan					
Out-of-bounds Read	02-Nov-20	6.4	<p>u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-SAIP-181120/1825

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
			Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1826

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
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1827

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
			SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1828
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1829

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
			Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1830
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3694	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1831

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
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1832

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
			CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1833
Buffer Copy without Checking	02-Nov-20	4.6	<p>u'Possible buffer overflow in MHI driver due to lack of input parameter validation</p>	https://www.qualcomm.com/c	H-QUA-SAIP-181120/1834

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
Size of Input ('Classic Buffer Overflow')			of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1835

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
			APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1836

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
			CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	<p>u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'</p> <p>in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11174</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SAIP-181120/1837
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow occurs while processing SIP message packet due to lack</p>	https://www.qualcomm.com/c	H-QUA-SAIP-181120/1838

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
			of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	company/product-security/bulletins/october-2020-bulletin	
ipq6018					
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ6-181120/1839

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
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrttr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ6-181120/1840

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
			MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ6-181120/1841

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
			SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ6-181120/1842
Out-of-bounds Write	02-Nov-20	7.5	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/b	H-QUA-IPQ6-181120/1843

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
			Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980 CVE ID : CVE-2020-11172	ulletins/oc tober-2020-bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ6-181120/1844
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ6-181120/1845

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	tober-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-IPQ6-181120/1846

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
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657		
kamorta					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1847

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
			IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1848

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
			QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1849
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1850

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	tober-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1851

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
			IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1852
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack	https://www.qualcomm.com/c	H-QUA-KAMO-181120/1853

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
			of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	company/product-security/bulletins/october-2020-bulletin	
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1854

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
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1855

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
			QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130 CVE ID : CVE-2020-3678	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1856
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1857

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
			Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1858

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
			SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1859
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-KAMO-181120/1860

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
			<p>Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</p> <p>CVE ID : CVE-2020-3703</p>		
Improper Input Validation	02-Nov-20	7.8	<p>u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-KAMO-181120/1861

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
			Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
bitra					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1862

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
			SM8250, SXR2130 CVE ID : CVE-2020-3638		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1863
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-BITR-181120/1864

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
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	2020-bulletin	
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1865

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
			QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3693	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1866
N/A	02-Nov-20	4.6	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1867

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
			CVE ID : CVE-2020-3694		
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1868

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
			CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1869

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
			SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1870
Buffer Copy without	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of	https://www.qualco	H-QUA-BITR-181120/1871

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
Checking Size of Input ('Classic Buffer Overflow')			input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	mm.com/company/product-security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1872

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
			Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1873

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
			SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-BITR-181120/1874
Improper Validation of	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://www.qualco	H-QUA-BITR-181120/1875

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
Array Index			<p>message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
qcs610					
Out-of-bounds Write	02-Nov-20	4.6	<p>u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1876

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
			<p>Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-11125</p>		
Use After Free	02-Nov-20	4.4	<p>u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019,</p>	<p>https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin</p>	H-QUA-QCS6-181120/1877

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
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1878
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1879

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
			check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	tober-2020-bulletin	
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1880

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
			MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1881

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
			MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1882
Buffer Copy without	02-Nov-20	10	u'Possible buffer overflow while updating output buffer	https://w www.qualco	H-QUA-QCS6-181120/1883

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
Checking Size of Input ('Classic Buffer Overflow')			for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3692	mm.com/company/product-security/bulletins/october-2020-bulletin	
Out-of-bounds Read	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overflow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1884

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
			MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCS6-181120/1885

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
			MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
sa8155p					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA81-181120/1886

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
			QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA81-181120/1887
Buffer Copy without Checking Size of Input ('Classic	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in	https://www.qualcomm.com/company/product-	H-QUA-SA81-181120/1888

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
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 APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA81-181120/1889

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
			SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA81-181120/1890
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-	H-QUA-SA81-181120/1891

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
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	2020-bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA81-181120/1892

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
			SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA81-181120/1893
Improper Validation of	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://www.qualco	H-QUA-SA81-181120/1894

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
Array Index			<p>message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2020-3654</p>	mm.com/company/product-security/bulletins/october-2020-bulletin	
Improper Validation of Array Index	02-Nov-20	10	<p>u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA81-181120/1895

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
			Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673		
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA81-181120/1896

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
			SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA81-181120/1897
sa515m					
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in	https://www.qualcomm.com/company/product-	H-QUA-SA51-181120/1898

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
			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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	security/bulletins/october-2020-bulletin	
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-SA51-181120/1899

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
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA51-181120/1900
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA51-181120/1901

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
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	tober-2020-bulletin	
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA51-181120/1902
Buffer Copy without Checking Size of Input ('Classic	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in	https://www.qualcomm.com/company/product-	H-QUA-SA51-181120/1903

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
Buffer Overflow')			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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	security/bulletins/october-2020-bulletin	
Integer Overflow or Wraparound	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' 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/october-2020-bulletin	H-QUA-SA51-181120/1904

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
			Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169		
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA51-181120/1905
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.'	https://www.qualcomm.com/company/p	H-QUA-SA51-181120/1906

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
			in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	product- security/b ulletins/oc tober- 2020- bulletin	
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SA51-181120/1907

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA51-181120/1908

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
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA51-181120/1909
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-SA51-181120/1910

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
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
mdm9645					
Out-of-bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-	H-QUA-MDM9-181120/1911

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
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, 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-2020-3670	bulletin	
qca4531					
Use After Free	02-Nov-20	4.6	u'Use after free while installing new security rule in ipcrt as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA4-181120/1912

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
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696		
qca6390					
Incorrect Default Permissions	02-Nov-20	4.6	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-3638	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1913
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to	https://www.qualcomm.com/company/product-	H-QUA-QCA6-181120/1914

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
			validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	security/bulletins/october-2020-bulletin	
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1915

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
			APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684		
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1916

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
			SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690		
Improper Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1917

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
			SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704		
Out-of-bounds Write	02-Nov-20	4.6	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1918
Improper	02-Nov-20	4.8	u'Buffer over-read issue in	https://w	H-QUA-QCA6-

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
Input Validation			Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	181120/1919
Out-of-bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1920
Buffer Copy without	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU	https://www.qualco	H-QUA-QCA6-181120/1921

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
Checking Size of Input ('Classic Buffer Overflow')			data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	mm.com/company/product-security/bulletins/october-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1922

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
			SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155		
Improper Input Validation	02-Nov-20	4.8	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1923
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in 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 Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1924

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
			IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11164	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1925
Integer Overflow or	02-Nov-20	6.4	u'Buffer over-read while processing received L2CAP	https://w www.qualco	H-QUA-QCA6-181120/1926

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
Wraparound			packet due to lack of integer overflow check' in Snapdragon Auto, 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, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	mm.com/company/product-security/bulletins/october-2020-bulletin	
Use After Free	02-Nov-20	4.4	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in 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 Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1927

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
			SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173		
Improper Validation of Array Index	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in 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 Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1928

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
			SXR1130, SXR2130 CVE ID : CVE-2020-11174		
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://www.qualcomm.com/company/product-security/bulletins/october-2020-bulletin	H-QUA-QCA6-181120/1929
Samsung					
exynos_990					
Buffer Copy without Checking Size of Input ('Classic	08-Nov-20	4.6	An issue was discovered on Samsung mobile devices with Q(10.0) (Exynos990 chipsets) software. The S3K250AF Secure Element	N/A	H-SAM-EXYN-181120/1930

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
Buffer Overflow')			CC EAL 5+ chip allows attackers to execute arbitrary code and obtain sensitive information via a buffer overflow. The Samsung ID is SVE-2020-18632 (November 2020). CVE ID : CVE-2020-28341		
exynos_980					
Out-of-bounds Write	08-Nov-20	4.6	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 980, 9820, and 9830 chipsets) software. The NPU driver allows attackers to execute arbitrary code because of unintended write and read operations on memory. The Samsung ID is SVE-2020-18610 (November 2020). CVE ID : CVE-2020-28343	N/A	H-SAM-EXYN-181120/1931
exynos_9820					
Out-of-bounds Write	08-Nov-20	4.6	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 980, 9820, and 9830 chipsets) software. The NPU driver allows attackers to execute arbitrary code because of unintended write and read operations on memory. The Samsung ID is SVE-2020-18610 (November 2020). CVE ID : CVE-2020-28343	N/A	H-SAM-EXYN-181120/1932
exynos_9830					
Out-of-	08-Nov-20	4.6	An issue was discovered on	N/A	H-SAM-EXYN-

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
bounds Write			Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 980, 9820, and 9830 chipsets) software. The NPU driver allows attackers to execute arbitrary code because of unintended write and read operations on memory. The Samsung ID is SVE-2020-18610 (November 2020). CVE ID : CVE-2020-28343		181120/1933
ZTE					
zxa10_eodn					
Information Exposure	05-Nov-20	4	A ZTE product is impacted by an information leak vulnerability. An attacker could use this vulnerability to obtain the authentication password of the handheld terminal and access the device illegally for operation. This affects: ZXA10 eODN V2.3P2T1 CVE ID : CVE-2020-6877	N/A	H-ZTE-ZXA1- 181120/1934

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