National Critical Information Infrastructure Protection CentreCommon Vulnerabilities and Exposures(CVE) Report							
Tools of NTVO	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		

0-1

1-2

2-3

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 Cryptographi c 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

0-1

1-2

2-3

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 Authorizatio n	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

0-1

1-2

4-5

5-6

6-7

7-8

8-9

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.		
Improper Access Control	05-Nov-20	9.3	CVE ID : CVE-2020-24432 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

0-1

1-2

2-3

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

0-1

1-2

2-3

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.		
Use After Free	05-Nov-20	6.8	CVE ID : CVE-2020-24436 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

0-1

1-2

2-3

<mark>3-4</mark>6

4-5

5-6

6-7

7-8

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	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- 181120/15
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- 181120/16
Time-of-	05-Nov-20	5.1	Acrobat Reader DC versions	N/A	A-ADO-ACRO-

0-1

<mark>3-4</mark> 7 4-5

5-6

2-3

1-2

7-8

6-7

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 Cryptographi c 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

0-1

1-2

2-3

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 Authorizatio n	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

0-1

1-2

9

2-3 3-4 4-5 5-6 6-7 7-8 8-9

			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- 181120/22
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- 181120/23
Heap-based Buffer	05-Nov-20	6.8	Acrobat Reader DC versions 2020.012.20048 (and	N/A	A-ADO-ACRO-

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.		181120/24
Out-of- bounds Write	05-Nov-20	6.8	CVE ID : CVE-2020-24435 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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Use After Free05-Nov-204.3Arabo-ACRO- tarier) 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. CVE ID : CVE-2020-24437N/AA-ADO-ACRO- 181120/27Use After Free05-Nov-204.3Acrobat Reader DC versions 2020.012.20048 (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-2020-24438N/AA-ADO-ACRO- 181120/27Out-of- bounds Read05-Nov-204.3Acrobat Reader DC versions 2020.012.00048 (and earlier) are affected by a use-after-free vulnerability that a victim must open a malicious file. CVE ID : CVE-2020-24438N/AA-ADO-ACRO- 181120/27Out-of- bounds Read05-Nov-204.3Acrobat Reader DC versions 2020.011.30005 (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 userN/A	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Image: constraint of the second sec				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.		
Out-of- bounds Read05-Nov-20A:3 A:3 A:3Acrobat 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 thisN/AA-ADO-ACRO- 181120/28		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	
Out-of- bounds Read05-Nov-200A-A2020.012.20048 (and earlier).2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by and 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 thisN/AA-ADO-ACRO- 181120/28	acrobat_read	er				
		05-Nov-20	4.3	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	N/A	

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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Cryptographi c 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 Authorizatio n	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

0-1

1-2

2-3

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

0-1

1-2

2-3

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-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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

0-1

1-2

2-3

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.		
acrobat_reade	er de		CVE ID : CVE-2020-24438		
Out-of-	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
	I				•

18

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 Cryptographi c 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

0-1

1-2

2-3

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 Authorizatio n	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

0-1

1-2

2-3

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

0-1

1-2

2-3

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

0-1

1-2

2-3

4-5

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	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- 181120/52
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. CVE ID : CVE-2020-24438	N/A	A-ADO-ACRO- 181120/53
Apache					
shiro					
Missing Authenticati on 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 Sca	ale 0-1	1-2	2-3 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		
Arubanetwor	ks				
airwave_glass	5				
Improper Neutralizatio n 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 Neutralizatio n 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_a	pplication_pa	ckage			
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

24

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					1
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	I			I	
anyconnect_s	ecure_mobilit	y_clier	nt		
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

0-1

1-2

2-3

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.						
Co lo oti ore			CVE ID : CVE-2020-27123						
Codection	waant waana a	nd av							
import_and_e	xport_users_a	ina_cu	stomers	1					
Improper Neutralizatio n 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	_syste	m						
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				
databasesche	maviewer_pr	oject							
databasesche	databaseschemaviewer								
Deserializati on 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://g hub.com/ martinjw dbschema reader/se curity/ad isories/G SA-rfjh-	/ A A-DAT-DATA- 2 181120/64 V				
CVSS Scoring Sca	le 0-1	1-2	2-3 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.	m356- mpqf	
			CVE ID : CVE-2020-26207		
droppy_proje	ct			1	
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 Neutralizatio n 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
easyregistrat	ionforms				
easy_registra					
Improper Neutralizatio n 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

Component ('Injection')Image: second	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
redcapImproper Neutralizatio n of Input During Web Page (Cross-site Scripting')02-Nov-203.5A 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-2020-27359N/AA-EVM-REDC- 181120/68F5big-ip_ssl_orchestratorN/A05-Nov-204.3In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0- 15.0.13, 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 failN/AA-F5-BIG 181120/69	Downstream Component ('Injection')			output from the forms information, there is no check on this inputs and the codes are executable.		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')02-Nov-203.5A 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 message could be used to perform this XSS attack. A user could craft a message and send it to anyone on the 	evms					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')02-Nov-203.5issue 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-2020-27359N/AA-EVM-REDC- 181120/68F5big-ip_ssl_orchestratorN/A05-Nov-204.3In versions 16.0.0-16.0.0.1, 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 failN/AA-F5-BIG 181120/69	redcap					
big-ip_ssl_orchestratorN/A05-Nov-204.3In 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 failN/AA-F5-BIG 181120/69	Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-20	3.5	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.	N/A	
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	F5					
N/A 05-Nov-20 4.3 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	big-ip_ssl_orc	hestrator				
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	N/A	05-Nov-20	4.3	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)	N/A	
	CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	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.	N/A	A-F5-BIG 181120/70
			CVE ID : CVE-2020-5943		
big-ip_access_	_policy_manag	ger			
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
I					
Improper Neutralizatio n 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

0-1

1-2

2-3

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 Neutralizatio n 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_advanc	ced_firewall_n	nanage	r	I	I
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

0-1

1-2

2-3

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 Neutralizatio n 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.	N/A	A-F5-BIG 181120/76
			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 181120/77
Improper Neutralizatio n 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

0-1

1-2

2-3

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_analyti	ics				
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 Neutralizatio n 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

0-1

1-2

2-3

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 Neutralizatio n 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_applica	tion accelera	tion m			
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 Neutralizatio n 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

0-1

1-2

2-3

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.	N/A	A-F5-BIG 181120/85
			CVE ID : CVE-2020-5943		
Improper Neutralizatio n 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_applica	ation_security	_mana	ger		
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

0-1

1-2

2-3

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 Neutralizatio n 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
			In versions 14.1.0-14.1.0.1		
Inadequate Encryption Strength	05-Nov-20	4	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 Neutralizatio n 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.	N/A	A-F5-BIG 181120/90
			CVE ID : CVE-2020-5945		

0-1

1-2

2-3

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	n_name_syste	m			•
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 Neutralizatio n 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

0-1

1-2

2-3

4-5

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 Neutralizatio n 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_g	ateway				
Improper Neutralizatio n 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_j	protection_se	rvice			
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 Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2020-5939					
Improper Neutralizatio n 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 Neutralizatio n 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_	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 Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	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 Neutralizatio n 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 Neutralizatio n 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

1-2

2-3

0-1

4-5

5-6

6-7

7-8

8-9

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_co	ontroller				
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 Neutralizatio n 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

0-1

1-2

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 Neutralizatio n 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_tr	raffic_manage	r			I
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 Neutralizatio	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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Neutralizatio n 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	manag	ger		
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

0-1

1-2

2-3

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 Neutralizatio n 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 Neutralizatio n 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

0-1

1-2

2-3

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_webaco	celerator				
Improper Neutralizatio n 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.	N/A	A-F5-BIG 181120/116
			CVE ID : CVE-2020-5940		
big-ip_advanc	ed_web_appli	ication	_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

0-1

1-2

2-3

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_h	ybrid_defend	er			
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

0-1

1-2

3-4 4-5 5-6 6-7 7-8 8-9 2-3 45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
foxit_reader	I			I	
N/A	02-Nov-20	6.8	Foxit Reader before 10.0 allows Remote Command Execution via the app.opencPDFWebPage JavsScript 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_pro	oject				
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_proje	ct			-1
git_large_file_	storage				
Improper Neutralizatio n 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				l	
chrome					
Use After	03-Nov-20	6.8	Use after free in payments in	N/A	A-GOO-CHRO-
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	<u>8 8-9 9-10</u>

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.		181120/124
			CVE ID : CVE-2020-15967		
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 in WebRTC in		
Use After Free	03-Nov-20	6.8	Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	N/A	A-GOO-CHRO- 181120/126
			CVE ID : CVE-2020-15969		
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.	N/A	A-GOO-CHRO- 181120/127
			CVE ID : CVE-2020-15970		
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

0-1

1-2

2-3

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	N/A	A-GOO-CHRO- 181120/130
			Chrome Extension.		
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

0-1

1-2

2-3

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

0-1

1-2

2-3

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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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

0-1

1-2

2-3

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.	N/A	A-GOO-CHRO- 181120/147
			CVE ID : CVE-2020-15990		
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

0-1

1-2

2-3

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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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

0-1

1-2

2-3

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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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

0-1

1-2

2-3

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.	N/A	A-GOO-CHRO- 181120/169
			CVE ID : CVE-2020-6557		
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://git hub.com/ hashicorp /consul/bl ob/master /CHANGE LOG.md#1 85- october- 23-2020	A-HAS-CONS- 181120/170
hcltech					
hcl_digital_ex	perience				
Improper Neutralizatio n 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

0-1

1-2

2-3

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				1
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</php_file_name>	N/A	A-HOR-HORI- 181120/172
synergy_com	noser				
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

0-1

1-2

2-3

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_com	poser_2			I	
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					I
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_d	eploy				
Incorrect Authorizatio n	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://w ww.ibm.co m/suppor t/pages/n ode/6337 603	A-IBM-URBA- 181120/176

0-1

1-2

2-3

4-5

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://w ww.ibm.co m/suppor t/pages/n ode/6360 835	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://w ww.ibm.co m/suppor t/pages/n ode/6337 605	A-IBM-URBA- 181120/178
planning_ana	lytics_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- privleged users by not invalidating TM1Web user sessions. IBM X-Force ID: 186022.	https://w ww.ibm.co m/suppor t/pages/n ode/6356 539	A-IBM-PLAN- 181120/179
			CVE ID : CVE-2020-4649		
filenet_conter	nt_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://w ww.ibm.co m/suppor t/pages/n ode/6336	A-IBM-FILE- 181120/180

CVSS Scoring Scale0-11-22-3

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.	917	
			CVE ID : CVE-2020-4759		
maximo_spat	ial_asset_man	ageme	nt		
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://w ww.ibm.co m/suppor t/pages/n ode/6361 769	A-IBM-MAXI- 181120/181
			IBM Maximo Spatial Asset		
Cross-Site Request Forgery (CSRF)	09-Nov-20	2.9	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://w ww.ibm.co m/suppor t/pages/n ode/6361 767	A-IBM-MAXI- 181120/182
app_connect_	enterprise_ce	rtified	_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://w ww.ibm.co m/suppor t/pages/n ode/6357 899	A-IBM-APP 181120/183
	le 0-1	1-2	2-3 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 Neutralizatio n 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 Neutralizatio n 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

0-1

1-2

2-3

4-5

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 Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-20	6	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.	N/A	A-IMM-IMMU- 181120/188
			CVE ID : CVE-2020-15952		
Jenkins					
vmware_lab_	manager_slav	es			
Unprotected Storage of Credentials	04-Nov-20	4	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. CVE ID : CVE-2020-2319	https://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2084	A-JEN-VMWA- 181120/189
mercurial					
Improper Restriction of XML External Entity Reference ('XXE')	04-Nov-20	4	Jenkins Mercurial Plugin 2.11 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. CVE ID : CVE-2020-2305	https://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2115	A-JEN-MERC- 181120/190
Missing Authorizatio n	04-Nov-20	4	A missing permission check in Jenkins Mercurial Plugin 2.11 and earlier allows	https://w ww.jenkin s.io/securi	A-JEN-MERC- 181120/191

0-1

1-2

2-3

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/advisor y/2020- 11- 04/#SECU RITY-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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-1646	A-JEN-KUBE- 181120/192
Missing Authorizatio n	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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2102	A-JEN-KUBE- 181120/193
Missing Authorizatio n	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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2103	A-JEN-KUBE- 181120/194
ansible					
Missing Authorizatio n	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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU	A-JEN-ANSI- 181120/195
CVSS Scoring Sca	le 0-1	1-2	2-3 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.	RITY-1943	
			CVE ID : CVE-2020-2310		
aws_global_co	onfiguration			L	
Missing Authorizatio n	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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2101	A-JEN-AWS 181120/196
sqlplus_script	t_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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2129	A-JEN-SQLP- 181120/197
azure_key_va	ult				
Missing Authorizatio n	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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU	A-JEN-APPS- 181120/199

0-1

1-2

2-3

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.	RITY-2058	
			CVE ID : CVE-2020-2314		
visualworks_s	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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-1900	A-JEN-VISU- 181120/200
findbugs	I			I	
Improper Neutralizatio n 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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-1918	A-JEN-FIND- 181120/201
mail_commar	ıder			I	
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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2085	A-JEN-MAIL- 181120/202
active_directo	ory				
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authenticati on	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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2117	A-JEN-ACTI- 181120/203
Improper Authenticati on	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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2099	A-JEN-ACTI- 181120/204
Improper Authenticati on	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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2123	A-JEN-ACTI- 181120/205
Missing Authorizatio n	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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-1999	A-JEN-ACTI- 181120/206
Cross-Site Request	04-Nov-20	4.3	A cross-site request forgery (CSRF) vulnerability in	https://w ww.jenkin	A-JEN-ACTI- 181120/207

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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/securi ty/advisor y/2020- 11- 04/#SECU RITY-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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-2145	A-JEN-SUBV- 181120/208
static_analysi	s_utilities				
Improper Neutralizatio n 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://w ww.jenkin s.io/securi ty/advisor y/2020- 11- 04/#SECU RITY-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_projec	joplin_project							
joplin								
Improper Neutralizatio n 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-chro	me-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-htm	l-to-ndf							
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					1			
play_framewo	ork							
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			

0-1

1-2

2-3

4-5

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
Linuxfoundat	tion				
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://ww w.openwal l.com/lists /oss- security/2 020/11/0 2/2	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://w ww.openw all.com/lis ts/oss- security/2 020/11/0 2/2	A-LIN-NATS- 181120/218
Magento					
magento					
Improper Neutralizatio n 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

0-1

1-2

2-3

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 Authorizatio n	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 Authorizatio n	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 Authorizatio n	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

0-1

1-2

2-3

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 Authorizatio n	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 Authorizatio n	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

0-1

1-2

2-3

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				1	
Improper Neutralizatio n 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

0-1

1-2

2-3

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	I			I	1
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

0-1

1-2

2-3

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 mosquitto executable is also run. CVE ID : CVE-2020-13537	N/A	A-MOX-MXVI- 181120/231
nedi					
nedi					
Improper Neutralizatio n 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 Neutralizatio n 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	l			L	
e-series_sant	ricity_os_cont	roller			
CVSS Scoring Sca	ale 0-1	1-2	2-3 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_p	assword_rese	et		1	
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
					l

CVSS Scoring Scale	0-1	1-2	2-3	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		
oleacorner					I
olea_gift_on_o	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 getfile.php?file=/ directory traversal. CVE ID : CVE-2020-9368	N/A	A-OLE-OLEA- 181120/238
openfind					<u> </u>
mailaudit					
Improper Neutralizatio n 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://w ww.twcert .org.tw/tw /cp-132- 4118- 6292c- 1.html	A-OPE-MAIL- 181120/239
mailgates					
Improper Neutralizatio n 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://w ww.twcert .org.tw/tw /cp-132- 4118- 6292c- 1.html	A-OPE-MAIL- 181120/240
Opensuse					I
backports_sle	•				

0-1

1-2

2-3

8-9

9-10

4-5

5-6

6-7

7-8

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

0-1

1-2

2-3

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

0-1

1-2

79

4-5

3-4

5-6

7-8

6-7

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

80

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_middl	eware				
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.	N/A	A-ORA-FUSI- 181120/257
			CVSS 3.1 Base Score 9.8		

81

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	1				
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.	N/A	A-OST-OSTI- 181120/258
****			CVE ID : CVE-2020-24881		
pega					
pega_platform	n				Т
Improper Neutralizatio n 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	l				·
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	<u> </u>				
-					

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipfs	L			L	
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				<u> </u>	
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://ww w.openwal l.com/lists /oss- security/2 020/11/0 3/2	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://ww w.openwal l.com/lists /oss- security/2 020/11/0 2/1	A-QEM-QEMU- 181120/263
robware					
rvtools					
Insufficiently Protected Credentials	05-Nov-20	5	RVToolsPasswordEncryptio n.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 Sca	le 0-1	1-2	2-3 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_man	ager				
Missing Authorizatio n	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 Authorizatio n	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.	N/A	A-SAP-SOLU- 181120/266
Missing			CVE ID : CVE-2020-26822 SAP Solution Manager (JAVA		
Authorizatio	10-Nov-20	6.4	stack), version - 7.20, allows	N/A	A-SAP-SOLU-

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.		181120/267
			CVE ID : CVE-2020-26823		
Missing Authorizatio n	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_ap	plication_ser	ver_jav	/a		
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	N/A	A-SAP-NETW- 181120/269
			availability of the server		

85

Execution using Shared Resource with Improper Synchronization ('Race Condition') Bilver-peak Improper Authenticati Improper Authenticati 05-Nov-20 Possible to log in to 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 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 N/A A-SDD-SDDM- 181120/270 A-SIL-UNIT- 181120/271	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	ו	NCIIP	CID
CVE ID : CVE-2020-26820sidesideSubmetric CVE-2020-26820Submetric CVE-2020-26820Submetric CVE-2020-26820Submetric CVE-2020-26820Submetric CVE-2020-26820Submetric CVE-2020-26820Concurrent Sung Shared Resource with Improper Synchronization (Race Condition')An issue was discovered in SDD before 0.19.0.1t incorrectly starts 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-2020-28049N/AA-SDD-SDDM- 181120/270Silver-peakSilver Peak Unity Orchestrator versions prior b 0.1+ uses HTTP headers to authenticate REST API calls from localhost. This makes it Authenticati on 0 cristator instances that are hosted by customers - on-premise or in a public cloud provider -are affectedN/AA-SIL-UNIT- 181120/271								
side side side side Silver peak 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. N/A A-SDD-SDDM- 181120/270 Silver-peak withy provider weystrokes or access the clipboard. This is caused by a race condition during Xauthority file creation. Silver-peak Wither provider weystrokes to authenticate REST API calls from localhost. This makes it possible to log in to Orchestrator by introducing an HTTP HOST headers to aut HTTP HOST headers et 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								
sddm Concurrent Execution using Shared Resource 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. N/A A-SDD-SDDM- 181120/270 Silver-peak U V V V Proper access the clipboard. This is caused by a race condition during Xauthority file creation. N/A A-SDD-SDDM- 181120/270 Silver-peak U V V V Proper access the clipboard. This is caused by a race condition during Xauthority file creation. N/A A-SDL-SDL-SDL-SDL-SDL-SDL-SDL-SDL-SDL-SDL	· · · ·			CVE ID : CVE-2020-20020				
Concurrent Execution using Shared Resource with Improper Condition')04-Nov-203.3An 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.N/AA-SDD-SDDM- 181120/270Silver-peak555 <td></td> <td>;</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>		;						
Concurrent Execution using Shared Resource with Improper Sonchronization (Race Condition')04-Nov-203.3SDDM 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, intercrept keystrokes or access the clipboard. This is caused by a race condition during Xauthority file creation. CVE ID : CVE-2020-28049N/AA-SDD-SDDM- 181120/270Silver-peakUUUSilver-PeakUSilver-peakUUOrchestrator 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 headers to authenticate rest possible to log in to Orchestrator instances that are hosted by customers - on-premise or in a public cloud provider -are affectedN/AA-SIL-UNIT- 181120/271	sddm							
Silver-peak unity_orchestrator Unity_orchestrator Unity_orchestrator Unity_orchestrator Unity_orchestrator Unity_orchestrator 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	Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	04-Nov-20	3.3	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	N/A			
unity_orchestrator unity_orchestrator Improper Authenticati on 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				CVE ID : CVE-2020-28049				
Improper Authenticati on05-Nov-207.5Silver 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 affectedN/AA-SIL-UNIT- 181120/271	Silver-peak							
Improper Authenticati on05-Nov-207.5Orchestrator 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 affectedN/AA-SIL-UNIT- 181120/271	unity_orchest	rator						
	Improper Authenticati on	05-Nov-20	7.5	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	N/A			
			4 2			-		

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				I	
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.	N/A	A-TCP-TCPD- 181120/274
			CVE ID : CVE-2020-8036		
Allocation of Resources Without Limits or	04-Nov-20	5	The ppp decapsulator in tcpdump 4.9.3 can be convinced to allocate a large amount of memory.	N/A	A-TCP-TCPD- 181120/275
Throttling			CVE ID : CVE-2020-8037		
Telerik					
fiddler					

0-1

1-2

2-3

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.	N/A	A-TEL-FIDD- 181120/276
			CVE ID : CVE-2020-13661		
web-audimex audimexee					
auuiiiiexee					
Improper Neutralizatio n 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 Neutralizatio n 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					<u> </u>
- F					

0-1

1-2

2-3

3-4

88

4-5

6-7

7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
weforms	L			L	
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	I			I	
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.	https://w ww.whats app.com/s ecurity/ad visories/2 020/	A-WHA-WHAT- 181120/280
			CVE ID : CVE-2020-1908		
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://w ww.whats app.com/s ecurity/ad visories/2 020/	A-WHA-WHAT- 181120/281
whatsapp_bu	siness				
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://w ww.whats app.com/s ecurity/ad	A-WHA-WHAT- 181120/282

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

	CVSS	Description & CVE ID	Patch	NCIIPC ID
		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/2 020/	
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://w ww.whats app.com/s ecurity/ad visories/2 020/	A-WHA-WHAT- 181120/283
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.	N/A	A-WIR-WIRE- 181120/284
		CVE ID : CVE-2020-28030		
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
	02-Nov-20	02-Nov-20 5	03-Nov-207.5permitted use of Siri to interact with the WhatsApp application even after the phone was locked.03-Nov-207.5A 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-2020-190902-Nov-205In Wireshark 3.2.0 to 3.2.7, the GQUIC dissector could crash. This was addressed in epan/dissectors/packet- gquic. by correcting the implementation of offset advancement. CVE ID : CVE-2020-2803002-Nov-207.5WordPress before 5.5.2 mishandles deserialization requests in wp-	03-Nov-207.5permitted use of Siri to interact with the WhatsApp application even after the phone was locked. CVE ID : CVE-2020-1908020/03-Nov-207.5A 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-2020-1909https://w www.whats app.com/s eurity/ad visories/2 020/02-Nov-205In 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-2020-28030N/A02-Nov-207.5WordPress before 5.5.2 mishandles deserialization requests in wp-N/A

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lteredIterator.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 Neutralizatio n 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

0-1

1-2

2-3

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 Neutralizatio n 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

0-1

1-2

2-3

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

0-1

1-2

2-3

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 Cryptographi c 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 Authorizatio n	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

0-1

1-2

2-3

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	N/A	O-APP-MAC 181120/300
			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	N/A	O-APP-MAC 181120/301

0-1

1-2

2-3

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	0-APP-MAC 181120/303

0-1

1-2

2-3

4-5

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	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	0-APP-MAC 181120/304
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-APP-MAC 181120/305
Use After Free	05-Nov-20	4.3	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005	N/A	O-APP-MAC 181120/306
CVSS Scoring Sca	le 0-1	1-2	2-3 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					I
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

0-1

1-2

2-3

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	I				
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 Synchronizat ion ('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
Fedoraprojec	it is a second s				
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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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.	N/A	O-FED-FEDO- 181120/313
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.	N/A	O-FED-FEDO- 181120/314
		CVE ID : CVE-2020-15969		
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
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
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
	03-Nov-20 03-Nov-20 03-Nov-20	03-Nov-20 6.8 03-Nov-20 6.8 03-Nov-20 6.8 03-Nov-20 6.8 03-Nov-20 6.8	03-Nov-206.8Use 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-2020-1596803-Nov-206.8Use 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.03-Nov-206.8Use 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.03-Nov-206.8Use 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.03-Nov-206.8Use 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.03-Nov-206.8Use 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.03-Nov-206.8Use 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.03-Nov-206.8Use after free in audio in Google Chrome prior to 86.0.4240.75 allowed a	03-Nov-206.8Use 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.N/A03-Nov-206.8Use 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.N/A03-Nov-206.8Use 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.N/A03-Nov-206.8Use 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.N/A03-Nov-206.8Use 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.N/A03-Nov-206.8Use 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.N/A03-Nov-206.8Use after free in audio 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.N/A03-Nov-206.8Use after free in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to poten

100

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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	0-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	0-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	0-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	0-FED-FEDO- 181120/326

0-1

1-2

2-3

<mark>3-4</mark> 102 4-5

5-6

7-8

6-7

9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		potentially exploit heap corruption via a crafted WebRTC stream.		
		CVE ID : CVE-2020-15987		
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
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
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
		L		1
10-Nov-20	2.1	In CellBroadcastReceiver's intent handlers, there is a possible denial of service due to a missing permission	N/A	0-GOO-ANDR- 181120/330
	03-Nov-20 03-Nov-20 03-Nov-20	Image: marked biase in the second	Image: construction of the second s	Image: constraint of the set

CVSS Scoring Scale 0-1	CVSS Scoring Scale	0-1
------------------------	--------------------	-----

1-2

2-3

4-5

5-6

6-7

3-4

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	0-G00-ANDR- 181120/332

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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- 140256621		
			CVE ID : CVE-2020-0439		
Uncontrolled Resource Consumption	10-Nov-20	7.8	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: AndroidVersions: Android- 11 Android-8.0 Android-8.1 Android-9 Android- 10Android ID: A-158304295	N/A	0-G00-ANDR- 181120/333
			CVE ID : CVE-2020-0441		
Improper Input Validation	10-Nov-20	7.8	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: AndroidVersions: Android- 10 Android-11 Android-8.0	N/A	0-G00-ANDR- 181120/334

0-1

1-2

2-3

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- 9Android 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	0-G00-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	0-G00-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	0-G00-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	0-G00-ANDR- 181120/338

0-1

1-2

2-3

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

107

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	N/A	O-GOO-ANDR- 181120/341		
			CVE ID : CVE-2020-0450				
Out-of- bounds Write	10-Nov-20	9.3	In sbrDecoder_AssignQmfChan nels2SbrChannels 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	0-G00-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							

108

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	0-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	0-GOO-ANDR- 181120/345

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android- 9Android 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	0-G00-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

0-1

1-2

110

2-3

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.	N/A	O-GOO-ANDR- 181120/350
			CVE ID : CVE-2020-15994		
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.	N/A	O-GOO-ANDR- 181120/351
			CVE ID : CVE-2020-15995		
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	0-G00-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

111

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).	N/A	0-GOO-ANDR- 181120/356
			CVE ID : CVE-2020-28340		
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).	N/A	0-GOO-ANDR- 181120/357
			CVE ID : CVE-2020-28341		
N/A	08-Nov-20	6.8	An issue was discovered on Samsung mobile devices	N/A	O-GOO-ANDR-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	0-G00-ANDR- 181120/359
imomobile					
verve_connec	t_vh510_firm	ware			
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

0-1

1-2

2-3

4-5

5-6

6-7

3-4

7-8

8-9

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 Neutralizatio n 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				1	
windows			1 60		
N/A	03-Nov-20	6.8	Insufficient policy enforcement in downloads	N/A	0-MIC-WIND- 181120/364
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 114	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	0-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

0-1

1-2

2-3

<mark>3-4</mark> 115 4-5

5-6

6-7

7-8

8-9

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.		
Time-of- check Time- of-use (TOCTOU) Race Condition	05-Nov-20	5.1	CVE ID : CVE-2020-24427 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	0-MIC-WIND- 181120/368
Improper Verification of Cryptographi c 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

0-1

1-2

2-3

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 Authorizatio n	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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	0-MIC-WIND- 181120/374

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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

0-1

1-2

2-3

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.	N/A	O-MIC-WIND- 181120/379
			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.	N/A	0-MIC-WIND- 181120/380
			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.	N/A	O-MIC-WIND- 181120/381

CVSS	Scoring	Scale	
------	---------	-------	--

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	0-MIC-WIND- 181120/385

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	0-MIC-WIND- 181120/388

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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.	N/A	O-MIC-WIND- 181120/389
			CVE ID : CVE-2020-17055		
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.	N/A	O-MIC-WIND- 181120/390
			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,	N/A	0-MIC-WIND- 181120/391

0-1

1-2

2-3

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.	N/A	O-MIC-WIND- 181120/392
			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- 181120/393
			Windows Remote Access		
Improper Privilege Management	11-Nov-20	4.6	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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		CVE-2020-17044, CVE-2020- 17055		
		CVE ID : CVE-2020-17027		
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- 181120/395
11-Nov-20	4.6	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.	N/A	O-MIC-WIND- 181120/396
		Windows Remote Access		
11-Nov-20	4.6	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
	11-Nov-20 11-Nov-20	Image: marked biase Image: marked biase 11-Nov-20 4.6 Image: marked biase Image: marked biase 11-Nov-20 4.6	Image: constraint of the second sec	Image: constraint of the second sec

0-1

1-2

2-3

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

0-1

1-2

2-3

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.	N/A	O-MIC-WIND- 181120/402
			CVE ID : CVE-2020-17055		
windows_rt_8	3.1				T
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	0-MIC-WIND- 181120/403
			Windows Remote Access		
Improper Privilege Management	11-Nov-20	4.6	Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020- 17025, CVE-2020-17027,	N/A	0-MIC-WIND- 181120/404

0-1

1-2

2-3

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.	N/A	O-MIC-WIND- 181120/405
			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.	N/A	O-MIC-WIND- 181120/406
			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-	N/A	O-MIC-WIND- 181120/407

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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.	N/A	O-MIC-WIND- 181120/408
			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- 181120/409
			Windows Remote Access		
Improper Privilege Management	11-Nov-20	4.6	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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Privilege Management 11-Nov-20 6.8 CVE-2020-17/027, CVE-2020-17/031, CVE-2020-17/032, CVE-2020-17/034, CVE-2020-17/034, CVE-2020-17/043 N/A 0-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-2020-17/031, CVE-2020-17/032, CVE-2020-17/034, CVE-2020-17/025, CVE-2020-17/026, CVE-2020-17/027, CVE-2020-17/031, CVE-2020-17/032, CVE-2020-17/034, CVE-2020-17/033, CVE-2020-17/034, CVE-2020-17/033, CVE-2020-17/034, CVE-2020-17/033, CVE-2020-17/034, CVE-2020-17/034, CVE-2020-17/034, CVE-2020-17/035, CVE-2020-17/034, CVE-2020-17/034, CVE-2020-17/034, CVE-2020-17/035, CVE-2020-17/034, CVE-2020-17/036, CVE-2020-17/034, CVE-2020-17/036, CVE-2020-17/034, CVE-2020-17/025, CVE-2020-17/026, CVE-2020-17/026, CVE-2020-17/026, CVE-2020-17/027, CVE-2020-17/026, CVE-2020-17/027, CVE-2020-17/026, CVE-2020-17/027, CVE-2020-17/026, CVE-2020-17/026, CVE-2020-17/026, CVE-2020-17/027, CVE-	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management11-Nov-20e.8Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17026, CVE-2020-17027, CVE-2020-17031, CVE-2020-17033, CVE-2020-17034, CVE-2020-17034, CVE-2020-17044, CVE-2020-17044, CVE-2020-17043, CVE-2020-17044, CVE-2020-17044, CVE-2020-17044, CVE-2020-17026, CVE-2020-17026, CVE-2020-17026, CVE-2020-17027, CVE-2020-17026, CVE-2020-17027, CVE-2020-17031, CVE-2020-17026, CVE-2020-17027, CVE-2020-17034, CVE-2020-17032, CVE-2020-17034, CV				CVE ID : CVE-2020-17034		
Improper Privilege Management11-Nov-200esseeElevation of Privilege Vulnerability This CVE ID is 17025, CVE-2020-17026, CVE-2020-17031, CVE-2020-17032, CVE-2020- 17033, CVE-2020-17034, CVE-2020-17034, CVE-2020-17043, CVE-2020- 17055.P/AO-MIC-WIND- 181120/412Improper Privilege Management11-Nov-2006.8Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17026, CVE-2020-17027, CVE-2020- 17055.N/AAImproper Privilege Management6.8Windows Remote Access Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2020-17026, CVE-2020-17027, CVE-2020- 17025, CVE-2020-17026, CVE-2020-17027, CVE-2020- 17033, CVE-2020-17034, CVE-2	Improper Privilege Management	11-Nov-20	6.8	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.	N/A	
Improper Privilege Management11-Nov-206.8Elevation 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.N/AO-MIC-WIND- 181120/413CVE ID : CVE-2020-17037, CVE-2020- 17033, CVE-2020-17034, CVE-2020-17034, CVE-2020-17044.O-MIC-WIND- 181120/413	Improper Privilege Management	11-Nov-20	6.8	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	
windows_server_2008	Improper Privilege Management	11-Nov-20	6.8	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.	N/A	
	windows_serv	ver_2008				

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	0-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_serv	ver_2012		1		
Improper	11-Nov-20	4.6	Windows Remote Access Elevation of Privilege	N/A	0-MIC-WIND- 181120/417

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	0-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	0-MIC-WIND- 181120/420

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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.	N/A	O-MIC-WIND- 181120/421
			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.	N/A	O-MIC-WIND- 181120/422
			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-	N/A	O-MIC-WIND- 181120/423

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9 **9-1**0

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.	N/A	O-MIC-WIND- 181120/424
			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.	N/A	O-MIC-WIND- 181120/425
			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.	N/A	O-MIC-WIND- 181120/426

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_serv	ver_2016				<u> </u>
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

0-1

1-2

4-5

5-6

6-7

7-8

8-9

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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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.	N/A	O-MIC-WIND- 181120/434
			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.	N/A	0-MIC-WIND- 181120/435
			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-	N/A	0-MIC-WIND- 181120/436

0-1

1-2

2-3

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.	N/A	O-MIC-WIND- 181120/437
			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.	N/A	O-MIC-WIND- 181120/438
windows_serv	vor 2010		CVE ID : CVE-2020-17055		
Window5_3CI	CI_2017		Windows Pomoto Access		
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

0-1

1-2

2-3

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.	N/A	O-MIC-WIND- 181120/440
			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- 181120/441
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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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-2020-17026, 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	0-MIC-WIND- 181120/446

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
Mitsubishiele					
mersec_iq-rj/	1eip91_firmw	are	Buffer overflow vulnerability		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	7.5	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 RD810PC96 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	0-MIT-MELS- 181120/451

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 RD810PC96 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,	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 RD810PC96 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 RD810PC96 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	0-MIT-MELS- 181120/453

0-1

1-2

2-3

3-4 145 4-5

5-6

6-7 7-8

8-9

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 RD810PC96 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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 RD810PC96 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-rj7	1pn92_firmw	are			
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 RD810PC96 0PC	N/A	O-MIT-MELS- 181120/456

0-1

1-2

2-3

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 RD810PC96 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	0-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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 RD810PC96 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	N/A	O-MIT-MELS- 181120/459
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Module First 2 digits of serial number are '04' or before, and RD810PC96 0PC 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 RD810PC96 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	0-MIT-MELS- 181120/460

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 RD810PC96 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	0-MIT-MELS- 181120/461
melsec ia-rd	81dl96_firmw	are			
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
without Checking Size of Input ('Classic Buffer		7.5	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	N/A 6-7 7-8	

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 RD810PC96 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 RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a	N/A	O-MIT-MELS- 181120/463

152

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 RD810PC96 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

0-1

1-2

2-3

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 RD810PC96 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	N/A	O-MIT-MELS- 181120/466

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Module First 2 digits of serial number are '04' or before, and RD810PC96 0PC 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		
Uncontrolled Resource Consumption	02-Nov-20	5	Resource ManagementErrors vulnerability inTCP/IP function included inthe firmware of MELSEC iQ-R series (RJ71EIP91EtherNet/IP NetworkInterface Module First 2digits of serial number are'02' or before, RJ71PN92PROFINET IO ControllerModule First 2 digits ofserial number are '01' orbefore, RD81DL96 HighSpeed Data Logger ModuleFirst 2 digits of serialnumber are '08' or before,RD81MES96N MES InterfaceModule First 2 digits ofserial number are '04' orbefore, and RD810PC96 OPCUA Server Module First 2digits of serial number are '04' orbefore, and RD810PC96 OPCUA Server Module First 2digits of serial number are'04' or before) allows aremote unauthenticatedattacker to stop the networkfunctions of the products viaa specially crafted packet. CVE ID : CVE-2020-5658	N/A	0-MIT-MELS- 181120/467

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9 **9-1**0

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
melsec_iq-rd	81mes96n_fir	mware		I	
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 RD810PC96 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	0-MIT-MELS- 181120/468
			CVE ID : CVE-2020-5653 Session fixation vulnerability		
Session Fixation	02-Nov-20	5	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	0-MIT-MELS- 181120/469

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 RD810PC96 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	CVEID: CVE-2020-3034NULL pointer dereferencesvulnerability in TCP/IPfunction included in thefirmware of MELSEC iQ-Rseries (RJ71EIP91EtherNet/IP NetworkInterface Module First 2digits of serial number are'02' or before, RJ71PN92PROFINET IO ControllerModule First 2 digits ofserial number are '01' orbefore, RD81DL96 HighSpeed Data Logger ModuleFirst 2 digits of serialnumber are '08' or before,RD81MES96N MES InterfaceModule First 2 digits ofserial number are '04' orbefore, and RD810PC96 OPCUA Server Module First 2digits of serial number are'04' or before) allows aremote unauthenticatedattacker to stop the network	N/A	O-MIT-MELS- 181120/470

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 RD810PC96 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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 RD810PC96 0PC 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		
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	N/A	O-MIT-MELS- 181120/473
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			serial number are '04' or before, and RD810PC96 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-rd	<mark>B1opc96_firm</mark>	ware			
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 RD810PC96 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

0-1

1-2

2-3

4-5

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 RD810PC96 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- 181120/475
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	N/A	O-MIT-MELS- 181120/476
CVSS Scoring Sca	ale 0-1	1-2	2-3 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 RD810PC96 0PC 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 RD810PC96 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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 10 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 RD810PC96 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. N/A 0-MIT-MELS- 181120/478 Uncontrolled Resource 02-Nov-20 5 Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iD0. N/A	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Argument Injection or ModificationImproper 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 '01' or before, RD81DL96 High NicationN/AO-MIT-MELS- 181120/478Argument Injection or Modification02-Nov-203.3Speed 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 RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before, and RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before, and RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before, and RD810PC96 OPC UA Server Module First 2 digits of serial number are index of the products via a specially crafted packet.O-MIT-MELS- 0-MIT-MELS-				via a specially crafted packet.		
Argument Injection or Modification02-Nov-20argument 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, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '04' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD810PC96 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.N/A0-MIT-MELS- 0-MIT-MELS- 0-MIT-MELS- 0-MIT-MELS- 0-MIT-MELS- 0-MIT-MELS-Uncontrolled Resource02-Nov-205Resource Management Errors vulnerability in TCP/IP function included in the network functions of the products via a specially crafted packet.N/A0-MIT-MELS-				CVE ID : CVE-2020-5656		
Uncontrolled Errors vulnerability in Uncontrolled TCP/IP function included in Resource 02-Nov-20 5 the firmware of MELSEC io N/A O-MIT-MELS-	Injection or	02-Nov-20	3.3	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 RD810PC96 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.	N/A	
Consumption Consumption R series (RJ71EIP91 EtherNet/IP Network 181120/479	Resource	02-Nov-20	5	Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ- R series (RJ71EIP91	N/A	O-MIT-MELS- 181120/479

0-1

1-2

2-3

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 RD810PC96 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_fir	mware				
Improper Neutralizatio n 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.	N/A	0-MOX-VPOR- 181120/480
			CVE ID : CVE-2020-23639		
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	0-OPE-LEAP- 181120/481
CVSS Scoring Sca	le 0-1	1-2	2-3 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	0-0PE-LEAP- 181120/485
Out-of-	03-Nov-20	6.8	Inappropriate	N/A	O-OPE-LEAP-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Synchronizat ion ('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_fi	rmware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/488

0-1

1-2

2-3

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, 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 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 Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/489

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/490
CVSS Scoring Sca	le 0-1	1-2	2-3 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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-QCA6- 181120/492

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, Snapdragon Wiela Snapdragon Wiearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9607, 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 	security/b ulletins/oc tober- 2020- bulletin	
qcs405_firmw	vare				
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 Consumer IOT, Snapdragon Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/493

0-1

1-2

2-3

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 Overfow 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 Consumer Electronics Connectivity,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/494
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

171

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, 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 Industrial IOT, Snapdragon Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/495

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, 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 Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/496

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8905, 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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/497

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/498
Improper Validation of	02-Nov-20	4.6	u'Array index underflow issue in adsp driver due to	https://w ww.qualco	0-QUA-QCS4- 181120/499

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Array Indeximproper check of channel id before used as array index.'mm.com/c ompany/p roduct- Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobilemm.com/c ompany/p roduct- security/b	111 /		CVSS	Publish Date	Weakness
Shapiragon Woote, buttern Snapdragon Voice & Music, Snapdragon Wiead 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, SDM630, SDM630, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	ndex.' ompany/p roduct- security/b vity, ulletins/oc r IOT, tober- 1 IOT, 2020- bulletin Ausic, es, ''''''''''''''''''''''''''''''''''''	before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, 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			Array Index
(1/2-NOV-/1) Use when Device configuration is company /n	YWW.qualcoYww.qualcoYmm.com/cation isompany/predroduct-versecurity/b	happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver	10	02-Nov-20	without Checking Size of Input ('Classic
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9	5-6 6-7 7-8 8-9 9-10	2-3 3-4 4-5 5-6	1-2	ale 0-1	CVSS Scoring Sca

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 Woice & 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, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	tober- 2020- bulletin	
ipq4019_firm	ware				
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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-IPQ4- 181120/501

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Out-of- bounds02-Nov-204.6Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ806401, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM92077, MSM8906AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Nov-204.6u'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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile,https://w www.qualco ompany/p roduct- 002-Nov-20Out-of- bounds02-Nov-204.6Snapdragon Wearables, Napdragon Wired Infrastructure and Networking in Agatti, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA4531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M,Ioteon				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		
	bounds	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 Wearables, 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, Rennell, SA415M, SA515M,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	• •

178

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		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	CVE ID : CVE-2020-11125 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 Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCX404, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ4- 181120/503

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ4- 181120/505
Improper	02-Nov-20	4.6	u'Array index underflow	https://w	0-QUA-IPQ4-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			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 Nobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/506
			CVE ID : CVE-2020-11174		
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://w ww.qualco mm.com/c ompany/p roduct- security/b	0-QUA-IPQ4- 181120/507
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Woice & 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	ulletins/oc tober- 2020- bulletin	
ipq8064_firm	ware				
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ8- 181120/508

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

8-9 **9-1**0

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, 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 Industrial IOT, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ8- 181120/509

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	CVE ID : CVE-2020-11125 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Wired Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ8- 181120/510
			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		

0-1

1-2

2-3

4-5

5-6

6-7 7-8

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ8- 181120/512

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Improper Validation of Array Indexu'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Music, Snapdragon Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, PQ8093, APQ8093, APQ8017, arge0098, Brue, IPQ5018, IPQ6018, IPQ8064, IPQ5018, IPQ6018, IPQ8064, IPQ5018, IPQ6018, IPQ8064, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, IPQ8074, Kamorta, <th>Weakness</th> <th>Publish Date</th> <th>CVSS</th> <th>Description & CVE ID</th> <th>Patch</th> <th>NCIIPC ID</th>	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input02-Nov-2010happen by sending a carefully crafted POST query 	Validation of	02-Nov-20	4.6	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 Nobile, Snapdragon Woice & 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	
accessed from a tethered roduct-	without Checking	02-Nov-20	10	happen by sending a carefully crafted POST query	ww.qualco mm.com/c	e e

186

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 Nobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657 	security/b ulletins/oc tober- 2020- bulletin	
ipq8074_firm	ware				
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-IPQ8- 181120/515

0-1

1-2

2-3

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 Mobile, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ8- 181120/516

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wierables, Snapdragon Wierd 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ8- 181120/517

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ8- 181120/519

0-1

1-2

2-3

4-5

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	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 Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c	0-QUA-IPQ8- 181120/521

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Mobile, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
qca6174a_fir	mware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	O-QUA-QCA6- 181120/522

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632	bulletin	
Out-of- bounds Read	02-Nov-20	7.5	CVE ID : CVE-2020-11157 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/523
			Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,		

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8917, MSM8937, MSM8940, 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/524

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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_firm	iware				
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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Conpute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA9- 181120/525

0-1

1-2

2-3

4-5

5-6

6-7

3-4

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, 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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA9- 181120/526

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firm	iware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-QCA9- 181120/527
sdm429w_fir	mware				
Out-of- bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing	https://w ww.qualco	0-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, MDM9205, MDM9206, MDM9640, MDM9645, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	mm.com/c ompany/p 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	0-QUA-SDM4- 181120/529
CVSS Scoring Sca					

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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, 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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/530

0-1

1-2

2-3

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 Woice Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM896AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/532

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
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 Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/533

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

			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 u'Third-party app may also call the broadcasts in		
N/A 02	2-Nov-20	4.6	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM4- 181120/534
Jse After 02	2-Nov-20	4.4	u'Two threads running	https://w	O-QUA-SDM4-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Wired	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM4- 181120/536

0-1

1-2

2-3

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, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM4- 181120/537

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')02-Nov-20Nicobar, QCA6390, QCA6574AU, QCM215, Rennell, SA6155P, SA8155P, SA8155P, Sajpan, SDM430, SDM630, SDM632, SDM430, SDM630, SDM632, SDM430, SDM630, SDM632, SDM450, SDM630, SDM630, SDM632, SDM7150, SM8150, SM8250, SXR1130, SXR2130Https://w www.gualco mm.com/c ompany/p roduct- scurefully crafted P0ST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Nuetworking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9050, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8906AU, QCS610, QR85165, SC8180X, SDM620, SDM429, SDM429, SDM429, SDM429W,0-QUA-SDM4- scurity/b ultims/cure accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8906AU, QCS610, QR85165, SC8180X, SDA660, SDA845, SDM429, SDM429, SDM429W,0-QUA-SDM4- start and start and	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')02-Nov-2010happen 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile,https://w ww.qualco mm.com/c ommant/pBuffer Copy without Checking Size of Input ('Classic Buffer Overflow')02-Nov-201010https://w Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9620, MDM9206, MDM9206, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8905W, MSM8953, MSM89				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		
	without Checking Size of Input ('Classic Buffer	02-Nov-20	10	happen by sending acarefully crafted POST querywhen Device configuration isaccessed from a tetheredclient through webserverdue to lack of array boundcheck.' in Snapdragon Auto,Snapdragon Compute,Snapdragon Nobile,Snapdragon Nobile,Snapdragon WiredInfrastructure andNetworking in APQ8009,APQ8017, APQ8053,APQ8074, MDM9150,IPQ4019, IPQ6018, IPQ8064,IPQ8074, MDM9207C,MDM9650, MSM8905,MSM8996AU, QCA6574AU,QCS405, QCS610, QRB5165,SC8180X, SDA660, SDA845,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	÷

205

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_firmv	vare				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC71- 181120/539
Out-of- bounds Read	02-Nov-20	6.4	CVE ID : CVE-2020-3638 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC71- 181120/540

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, 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, 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC71- 181120/541

0-1

1-2

2-3

4-5

5-6

6-7

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC71- 181120/542
Buffer Copy without	02-Nov-20	10	u'Possible buffer overflow while updating output buffer	https://w ww.qualco	0-QUA-SC71- 181120/543

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
			CVE ID : CVE-2020-3692		
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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC71- 181120/544

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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_firm	nware				
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, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCM6- 181120/545

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 u'Possible buffer overflow		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCM6- 181120/546
			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 Overfow issue	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	O-QUA-QCM6- 181120/547

0-1

1-2

2-3

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 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, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	O-QUA-QCM6- 181120/548

212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VE-2019-19193) mentioned	bulletin	
			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		
apq8009_firm	iware				
			u'QSEE reads the access	https://w	
			permission policy for the	ww.qualco	
N/A	02-Nov-20	4.6	SMEM TOC partition from	mm.com/c	0-QUA-APQ8-
11/11	02 1107 20	1.0	the SMEM TOC contents	ompany/p	181120/549
			populated by XBL Loader	roduct-	
			and applies them without	security/b	

CVSS Scoring Scale 0-1 1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

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 Vired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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, SDM630, 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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-APQ8- 181120/550

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-QUA-APQ8- 181120/552

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SUM6125, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	O-QUA-APQ8- 181120/553

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wieed & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/554

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-APQ8- 181120/556

0-1

1-2

2-3

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/557

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-APQ8- 181120/558
			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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-APQ8- 181120/559

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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, 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-APQ8- 181120/560

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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		
apq8098_firm	ware		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, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/561

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 Consumer IOT, 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, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/562

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/563
Improper Restriction of Operations within the Bounds of a Memory	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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	O-QUA-APQ8- 181120/564

0-1

1-2

2-3

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 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/565
N/A	02-Nov-20	4.6	u'Third-party app may also call the broadcasts in	https://w ww.qualco	0-QUA-APQ8- 181120/566

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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/c ompany/p roduct- security/b 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/567

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
Improper Validation of Array Index	02-Nov-20	10	CVE ID : CVE-2020-11174 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/568

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

Size of Input 02-Nov-20 10 Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, 183	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
LendLe				SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')02-Nov-2010happen 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wierd Infrastructure and Size of Input ('Classic Buffer Overflow')https://w ww.qualco mm.com/c ompany/p roduct- security/b IPQ4019, IPQ6018, IPQ8063, MDM9206, MDM9207C, MDM9206, MDM9207, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8906AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDM45, SDX20,0-0 total total total total total total total total				CVE ID : CVE-2020-3654		
CVE ID : CVE-2020-3657	without Checking Size of Input ('Classic Buffer Overflow')		10	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 Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDM660, SDM845, SDX20,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-APQ8- 181120/569
msm8953_firmware	msm8953_fir	mware				
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8	CVSS Scoring Sci	ale0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, 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, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/570
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://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-MSM8- 181120/571
CVSS Scoring Scal	le 0-1	1-2	2-3 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, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	security/b 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 Overfow 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/572

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, 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/573

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8905, 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 Industrial IOT, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MSM8- 181120/574

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, Snapdragon Nobile, 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, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b	O-QUA-MSM8- 181120/576

0-1

1-2

2-3

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 Woice & 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 Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/577

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/578

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, Snapdragon Wiete Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/579

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
msm8998_fir	mware			1	
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, MSM8917, MSM8940, MSM8917, MSM8940, MSM8917, MSM8940, MSM8917, MSM8940, MSM8917, MSM8940, MSM8917, MSM8940, MSM8917, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/580
			u'Potential out of bounds	https://w	
Out-of- bounds Read	02-Nov-20	6.4	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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-MSM8- 181120/581

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM898, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA429W, SDM439, SDM429W, SDM439, SDM636, SDM660, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MSM8- 181120/582

0-1

1-2

2-3

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_firm	ware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-NICO- 181120/583

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130		
			CVE ID : CVE-2020-3670 u'Buffer overflow can		
Improper Validation of Array Index	02-Nov-20	10	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-NICO- 181120/584

0-1

1-2

2-3

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Noice & 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, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-NICO- 181120/585

0-1

1-2

2-3

4-5

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 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, SDM670, SDM710, SM8450, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-NICO- 181120/586
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-NICO- 181120/587

0-1

1-2

2-3

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b	O-QUA-NICO- 181120/590

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE is equivalent to Link Layer Length Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, 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, SDM710, SDM845, SDX20, SDM710, SDM845, SDX20, SDM710, SXR1130	ulletins/oc tober- 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	0-QUA-NICO- 181120/591

244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, 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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, 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://w ww.qualco mm.com/c ompany/p roduct- security/b	0-QUA-NICO- 181120/592

0-1

1-2

2-3

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-NICO- 181120/593

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

			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,		
			SDM439, SDM430, SDM032, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162		
N/A 0	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-NICO- 181120/594

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	0-QUA-NICO- 181120/596

0-1

1-2

2-3

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, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	tober- 2020- bulletin	
apq8053_firm	iware				
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 Wired Infrastructure and	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-APQ8- 181120/597

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

8-9

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 Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Wired Infrastructure and Networking in APQ8009,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-APQ8- 181120/599

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-APQ8- 181120/600
			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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/601

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-QUA-APQ8- 181120/603

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-APQ8- 181120/604

0-1

1-2

2-3

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, SDM429W, SDM439,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/605

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSS	Description & CVE ID SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654 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 Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://w	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	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, 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/606
Out-of- bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing	https://w ww.qualco	0-QUA-APQ8- 181120/607

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SM7150, SM8150, SDX20, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	mm.com/c ompany/p 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	O-QUA-APQ8- 181120/608
			1 0 ,	,	

256

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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, 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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/609

0-1

1-2

2-3

4-5

5-6

6-7

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/611

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-APQ8- 181120/612

0-1

1-2

2-3

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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM7150, SM8150,		
mdm9207c_fi	rmware				
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MDM9- 181120/613

0-1

1-2

2-3

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/614

0-1

1-2

2-3

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, 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 Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MDM9- 181120/615

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_fir	mware			1	
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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM660, SDM670, SDM710, SDM845, SDM850,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/616

0-1

1-2

2-3

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b	0-QUA-MSM8- 181120/618

0-1

1-2

2-3

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, 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, SDM650, SDX20, SXR1130, SXR2130 CVE ID : CVE-2020-3684	ulletins/oc tober- 2020- bulletin	
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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/619

0-1

1-2

2-3

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		
Out-of- bounds Read	02-Nov-20	7.5	CVE ID : CVE-2020-3696 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8937, MSM8940,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/620

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Out-of- bounds02-Nov-204.6MSM8953, Nicobar, QCA6174A, QCA9377, QCX2150, QCX6125, QCS610, QW215, Rennell, SC8180X, SDM429, SDM630, SDM632, SDM430, SDM632, SDM630, SDM632, SDM350, SDM630, SDM632, SDM310, SDM710, SDM845, SDX20, SDW710, SDM845, SDX24, SM6150, SM7150, SM8150, SXR1130Https://w www.qualco mm.com/c orpany/p roduct- Napdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8074, Kamorta, MDM9650, MSM8905, SMSM8917, MSM8953, Nicobar, QCA931, QCX150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennel, SA8155P, Salapan, SC8180X, SDM429,0-QUA-MSM8- IS1120/621	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Nov-204.6happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA4155P, SA8155P, Saipan,https://w https://w ww.qualco mm.com/c oduct- security/b				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		
	bounds	02-Nov-20	4.6	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 Mobile, Snapdragon Mobile, Snapdragon Wearables, 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-

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 Industrial IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-MSM8- 181120/623

0-1

1-2

2-3

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, APQ8053, APQ8096AU, APQ8074, Kamorta, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM632, SDM636, SDM660, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/624

0-1

1-2

2-3

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, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654		
			u'Remote code execution can		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	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 Comsumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/625

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firm	iware				
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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-QCN7- 181120/627

271

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 Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCN7- 181120/629

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCN7- 181120/630
			CVE ID : CVE-2020-11156		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-QUA-QCN7- 181120/631

0-1

1-2

2-3

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	2020- bulletin	
Improper Input Validation	02-Nov-20	7.8	CVE ID : CVE-2020-11169 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCN7- 181120/632

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firm	ware				
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, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM8- 181120/633

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

nnell, SA415M, Saipan, 7180, SC8180X, SDA660, A845, SDM429, M429W, SDM439, M450, SDM630, SDM632, M636, SDM660, SDM670, M710, SDM845, SDM850, X20, SDX24, SDX55, I6150, SM7150, SM8150, R1130 E ID : CVE-2020-3670		
E ID : CVE-2020-3670		
Buffer overflow can ppen as part of SIP essage packet processing nile storing values in array e to lack of check to lidate the index length' in apdragon Auto, apdragon Compute, apdragon Connectivity, apdragon Consumer IOT, apdragon Industrial IOT, apdragon Mobile, apdragon Wearables in atti, APQ8053, Q8096AU, APQ8098, tra, Kamorta, MSM8905, SM8909W, MSM8917, SM8940, MSM8953, SM8996AU, Nicobar, A6390, QCA6574AU, SM8996AU, Nicobar, A6390, QCA6574AU, SM8996AU, Nicobar, A6390, QCA6574AU, SM2150, QCS605, QM215, nnell, SA6155P, SA8155P, ipan, SDA660, SDM429, M429W, SDM439, M450, SDM630, SDM632.	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM8- 181120/634
e til ap ap ap ap ap ap ap ap ap ap ap ap ap	sage packet processing e storing values in array to lack of check to late the index length' in odragon Auto, odragon Compute, odragon Connectivity, odragon Consumer IOT, odragon Industrial IOT, odragon Mobile, odragon Wearables in ti, APQ8053, 3096AU, APQ8098, I, Kamorta, MSM8905, 3909W, MSM8917, 3940, MSM8953, 3996AU, Nicobar, 5390, QCA6574AU, 2150, QCS605, QM215, nell, SA6155P, SA8155P, an, SDA660, SDM429,	sage packet processing e storing values in array to lack of check to ate the index length' in odragon Auto, odragon Compute, odragon Connectivity, odragon Industrial IOT, odragon Mobile, odragon Wearables in ti, APQ8053, 8096AU, APQ8098, b, Kamorta, MSM8905, 8909W, MSM8917, 8940, MSM8953, 8996AU, Nicobar, 6390, QCA6574AU, 2150, QCS605, QM215, hell, SA6155P, SA8155P, an, SDA660, SDM429, 429W, SDM439, 450, SDM630, SDM632, 636, SDM660, SDM670, 710, SDM845, SM6150, 150, SM8150, SM8250,

0-1

1-2

2-3

<mark>3-4</mark> 276 4-5

6-7

5-6

8-9

7-8

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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM8- 181120/635
			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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM8- 181120/636

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	0-QUA-SDM8- 181120/638

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Improper Input Validation02-Nov-207.8Zayer Length Overflow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Noice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207, MDM9607, MSM8905, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM210, SDM630, SDM632, SDM210, SDM630, SDM632, SDM210, SDM630, SDM632, SDM210, SDM630, SDM632, SDM210, SDM630, SDM632, SDM210, SDM630, SDM632, SDM24, SM150, SMR130https://w www.qualco mm.com/c mmproper linput Validation02-Nov-207.8u'While processing invalid connection request PDI which is nonstandard mm.com/c improper linput Validationhttps://w www.qualco mm.com/c improper input vialidation0-QUA-SDM8- 181120/639	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation02-Nov-207.8connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE isww.qualco mm.com/c ompany/p roduct- ulletins/oc0-QUA-SDM8- 181120/639				(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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	2020-	
	Input	02-Nov-20	7.8	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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	•
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CVSS Scoring Sca	le <u>0-1</u>	1-2	2-3 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(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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, 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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	O-QUA-SDM8- 181120/640

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wieed 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM8- 181120/641

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM8- 181120/642

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM8- 181120/643

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, Snapdragon Nobile, Snapdragon Wierd Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8906AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM8- 181120/644		
apq8076_firmware							
Out-of-	02-Nov-20	7.5	u'Buffer over-read issue in Bluetooth peripheral	https://w ww.qualco	O-QUA-APQ8-		
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

bounds ReadRamon and the second of the second o	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper 02-Nov-20 5 unexpected control ww.qualco 181120/646	bounds Read			check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overfow 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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, 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	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/645
		02-Nov-20	5	unexpected control	ww.qualco	• •

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			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 Industrial IOT, 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	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
ipq5018_firm	ware				
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 Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-IPQ5- 181120/647

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

8-9

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, 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		
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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ5- 181120/648

0-1

1-2

2-3

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, 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 Industrial IOT, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ5- 181120/649

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ5- 181120/650
	02-Nov-20	4.6	u'Array index underflow	https://w	O-QUA-IPQ5-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of			issue in adsp driver due to	ww.qualco	181120/651
Array Index			improper check of channel id	mm.com/c	
			before used as array index.'	ompany/p	
			in Snapdragon Auto,	roduct-	
			Snapdragon Compute,	security/b	
			Snapdragon Connectivity,	ulletins/oc	
			Snapdragon Consumer IOT,	tober-	
			Snapdragon Industrial IOT,	2020-	
			Snapdragon Mobile,	bulletin	
			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		
apq8017_firm	iware				
			ulles out of your to be been	httm - //	
Improper			u'Use out of range pointer	https://w	O-QUA-APQ8-
Restriction	02-Nov-20	4.6	issue can occur due to	ww.qualco	181120/652
of			incorrect buffer range check	mm.com/c	101120/032
Operations			during the execution of	ompany/p	

0-1

1-2

2-3

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	roduct- security/b ulletins/oc tober- 2020- bulletin	
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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/653

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial 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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/654

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/655
Buffer Copy without	02-Nov-20	10	u'Remote code execution can happen by sending a	https://w ww.qualco	0-QUA-APQ8- 181120/656
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

293

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 Wearables, 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, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
			CVE ID : CVE-2020-3657		
apq8096au_fi	rmware			I	
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-QUA-APQ8- 181120/657

0-1

1-2

2-3

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/658

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
Improper Validation of Array Index	02-Nov-20	10	CVE ID : CVE-2020-11174 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/659

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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	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 Wearables, 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, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/660
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://w ww.qualco mm.com/c ompany/p roduct- security/b	0-QUA-APQ8- 181120/661

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/662

0-1

1-2

2-3

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, 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 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 Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8996AU, QCA4531,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-APQ8- 181120/663

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24		
			CVE ID : CVE-2020-3696		
sda845_firmv	vare				
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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b	0-QUA-SDA8- 181120/665

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Voice & Music, Snapdragon Wiearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8058, 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	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 Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDA8- 181120/666

0-1

1-2

2-3

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDA8- 181120/667

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-SDA8- 181120/669

0-1

1-2

2-3

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, 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 Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDA8- 181120/670
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

304

Improper Input02-Nov-207.8Rennell, SA415M, SA515M, SA6155P, SA8155P, Sagpan, SC7180, SC8180X, SDA845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130Network SM250, SXR1130, SXR2130Improper InputuWhile 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 swepttooth paper)' in Snapdragon Consumer Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Snapdragon Industrial IOT, Snapdragon Nireet Imfrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA63977, QCA9886, QCM6125, QCX7605, QCS404, QCS405, QCS605,0-QUA-SDA8- state state	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation02-Nov-2007.86 connection (normal source of the source of				SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
	Input	02-Nov-20	7.8	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 Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6574AU, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	č

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_firm	ware			I	I
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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/672

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p	O-QUA-SDM6- 181120/674

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, 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, SDM630, SDM20, SM7150, SM8150, SM8250, SXR1130, SXR2130	roduct- security/b ulletins/oc tober- 2020- bulletin	
			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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE-	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/675

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/676

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/677
CVSS Scoring Sca	le 0-1	1-2	2-3 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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c	0-QUA-SDM6- 181120/679

0-1

1-2

2-3

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 Nobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
sdm670_firm	ware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	O-QUA-SDM6- 181120/680

0-1

1-2

2-3

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, MSM898, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/681
CVSS Scoring Sca	le 0-1	1-2	2-3 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/683

0-1

1-2

2-3

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, 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, SM7150, SM8150, SM8250, SXR1130, SXR2130		
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 Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/684

0-1

1-2

2-3

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/685
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Improper Input Validation02-Nov-207.8SDM 450, SDM 630, SDM 630, SDM 630, SDM 640, SDM 20, SDM 710, SDM 845, SDX 20, SM 8150, SXR1130https://w wikich 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 swaptortb paper)' in Snapdragon Consumer Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial 10T, Snapdragon Noice & Mobile, Snapdragon Noice & Music, Snapdragon Voice & Music, Snapdragon	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation02-Nov-207.8Improper 7.8u'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 Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Input Validationhttps://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- builetin0-QUA-SDM6- 181120/686Improper Input Validation7.87.8Napdragon Consumer Snapdragon Consumer Snapdragon Consumer Infrastructure and Networking in Agatti, APQ8003, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, QCA6174A, QCA6390, QCA6574AU, QCS405, QCS610, QRB5165, Rennell,0-QUA-SDM6- security/b ulletins/oc tober- 2020- builetin				SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150,		
Improper Input Validation02-Nov-207.87.8connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into 				CVE ID : CVE-2020-3703		
	Input	02-Nov-20	7.8	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 Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS404, QCS405, QCS605,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	č

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/687
CVSS Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

318

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/689

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/690

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firm	ware				
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, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM7- 181120/691

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Consumer IOT, 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, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM7- 181120/692
Buffer Copy without	02-Nov-20	4.6	u'A buffer overflow could occur if the API is	https://w ww.qualco	0-QUA-SDM7- 181120/693

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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/c ompany/p roduct- security/b ulletins/oc 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM7- 181120/694
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 323	6-7 7-8	8-9 9-10

323

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 Industrial IOT, Snapdragon Woice & 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, SDM670, SDM710, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM7- 181120/695
			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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE-	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM7- 181120/696

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM7- 181120/697
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 325	6-7 7-8	8-9 9-10

325

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SUM6125, 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		
Out-of- bounds Write	02-Nov-20	4.6	CVE ID : CVE-2020-3704 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM7- 181120/698

0-1

1-2

2-3

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, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
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 Wearables, Snapdragon Wired Infrastructure and Networking in Agatti,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM7- 181120/699

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	CVE ID : CVE-2020-11162u'Third-party app may alsocall the broadcasts inPerfdump and causeprivilege escalation issuedue to improper accesscontrol' in Snapdragon Auto,Snapdragon Connectivity,Snapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon Mobile,Snapdragon Wearables inAgatti, APQ8096AU,APQ8098, Bitra, Kamorta,MSM8909W, MSM8917,MSM8940, Nicobar,QCA6390, QCM2150,QCA6390, QCM2150,QCA6390, QCM2150,SDM429W, SDM450,SDM630, SDM636, SDM660,SDM630, SDM636, SDM660,SDM670, SDM710, SM6150,SM7150, SM8150, SM8250,SXR1130, SXR2130CVE ID : CVE-2020-11164	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM7- 181120/700

2-3

0-1

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	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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM7- 181120/701
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	https://w ww.qualco mm.com/c ompany/p roduct-	O-QUA-SDM7- 181120/702

329

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, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	security/b ulletins/oc tober- 2020- bulletin	
sm6150_firm	ware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SM61- 181120/703

0-1

1-2

2-3

4-5

5-6

6-7

3-4

8-9

7-8

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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM61- 181120/704

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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	https://w ww.qualco mm.com/c ompany/p roduct- security/b	0-QUA-SM61- 181120/706
			validation' in Snapdragon Auto, Snapdragon Compute,	ulletins/oc tober-	

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

N/A02-Nov-207.2Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Vice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9205, MDM9205, MDM9950, MDM9205, MDM9950, MDM9205, MDM9950, MDM9205, MDM9950, MDM9205, MDM9950, MDM9205, MDM9950, MDM9205, MDM9206, MDM9604, RAMBARS, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM660, SDM660, SDM670, SDM710, SDM845, SDM630, SDM630, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDM850, SDX25, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130Https://w ww.qualco mm.com/c ompromise the hypervisor' in Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390,200VXSS Scoring Scate811223344556677889910	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/AO2-Nov-207.2configuration, the modemIHtps://wN/AO2-Nov-207.2compromise the hypervisormm.com/cSnapdragon Auto,mm.com/cmm.com/cSnapdragon Compute,ompany/pompany/pSnapdragon Consumer IOT,security/b181120/707Snapdragon Mobile,tober-181120/707Snapdragon Voice & Music,2020-1000-Snapdragon Wiredbulletin1000-Infrastructure andbulletin1000-Networking in Agatti, Bitra,infrastructure andinfrastructure andKamorta, Nicobar, QCA6390,infrastructure infrastructure andinfrastructure infrastructure andKamorta, Nicobar, QCA6390,infrastructure infrastructure infrastructure andinfrastructure infrastructure andKamorta, Nicobar, QCA6390,infrastructure infrastructure infr				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		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	N/A	02-Nov-20	7.2	configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-
	CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

333

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM61- 181120/709

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM61- 181120/710
			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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM61- 181120/711

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM61- 181120/712

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM61- 181120/713

0-1

1-2

2-3

4-5

5-6

6-7

Buffer Copy without Checking Size of Input (Classic Buffer Overflow')02-Nov-204.6Nicobar, QCA6390, QCA9331, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QR85165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Sagian, SCB180X, SDM429, SDM450, SDM432, SDM460, SDM470, SDM453, SDM450, SM710, SDM470, SDM454, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130https://w www.qualco of EOT events received from MHI device side' in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, SNB4557, Agensen, APQ8009, Bitra, IPQ8019, IPQ8014, IPQ8014, IPQ8014, IPQ8014, IPQ8014, IPQ8014, IPQ8014, IPQ80	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input 02-Nov-20Medical and the security of the s				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		
	without Checking Size of Input ('Classic Buffer	02-Nov-20	4.6	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 Mobile, Snapdragon Mobile, 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	e e

338

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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM61- 181120/715
			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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SM61- 181120/716

0-1

1-2

2-3

4-5

5-6

6-7

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, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130		
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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SM61- 181120/717

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM61- 181120/718

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130		
			CVE ID : CVE-2020-3654		
qm215_firmw	vare				
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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QM21- 181120/719

0-1

1-2

2-3

4-5

5-6

6-7 7-8

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QM21- 181120/720
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 Industrial IOT, Snapdragon Woile, Snapdragon Woile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-QM21- 181120/721

0-1

1-2

2-3

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, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QM21- 181120/722

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QM21- 181120/723

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, 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, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QM21- 181120/724
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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE-	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QM21- 181120/725

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firmw	are				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/726

0-1

1-2

2-3

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Wired Infrastructure and Networking in Agatti,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/728

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/729

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Overfow 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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8953, Nicobar, QCA6174A, QCA9377, QCA6174A, QCA9377, QCA2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/730

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Improper Input Validation02-Nov-207.8SM8150, SXR1130 CVE ID : CVE-2020-370302-Nov-207.802-Nov-207.802-Nov-207.87.8Stapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Noice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Noice & Music, Sna
Improper Input Validation02-Nov-207.8Improper Validation100-000-000-000-000-000-000-000-000-000
Improper Input02-Nov-207.8connection 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 Consumer Electronics Connectivity, Snapdragon Consumer Snapdragon Consumer Electronics Connectivity, Snapdragon IoT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Nired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ809, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9667, MDM9640, MDM9667, MDM9640, MDM9667, MDM9640, MDM9667, MDM9640, MDM967, CN7605, QCS610, QR5165, Rennell, SA415M, SA515M, Sapan, SC7180, SC3180X, SDA845, SDM660, SDM670, SDM210, SDM685, SDM50, SDX20,0-QUA-QCS4- security/b ultima is the structure and builterin
SDX24, SDX55, SM6150,

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 Nobile, Snapdragon Wieta 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, SDM429W, SDM439, SDM450, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/732
Improper	02-Nov-20	4.8	u'Buffer over-read issue in	https://w	0-QUA-QCS4-

0-1

1-2

2-3

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 Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/733
			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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/734

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS4- 181120/735
Improper	02-Nov-20	4.6	u'Array index underflow	https://w	0-QUA-QCS4-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of			issue in adsp driver due to	ww.qualco	181120/736
Array Index			improper check of channel id	mm.com/c	
			before used as array index.'	ompany/p	
			in Snapdragon Auto,	roduct-	
			Snapdragon Compute,	security/b	
			Snapdragon Connectivity,	ulletins/oc	
			Snapdragon Consumer IOT,	tober-	
			Snapdragon Industrial IOT,	2020-	
			Snapdragon Mobile,	bulletin	
			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		
sm8150_firm	ware				
			u'An Unaligned address or	https://w	
Incorrect			size can propagate to the	ww.qualco	0-QUA-SM81-
Default	02-Nov-20	4.6		mm.com/c	181120/737
Permissions			database due to improper		101120//0/
			page permissions and can	ompany/p	

0-1

1-2

2-3

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	roduct- security/b ulletins/oc tober- 2020- bulletin	
Out-of- bounds Read	02-Nov-20	6.4	CVE ID : CVE-2020-3638 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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM81- 181120/738

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 u'Buffer overflow can		
Improper Validation of Array Index	02-Nov-20	10	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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM81- 181120/739

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM81- 181120/740
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,	https://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-SM81- 181120/741

0-1

1-2

2-3

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/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c	0-QUA-SM81- 181120/743

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	ompany/p roduct- security/b 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM81- 181120/745

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDX20, SDM710, SDM845, SDX20, SDM24, SM6150, SM7150, SM8150, SXR1130		
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM81- 181120/746

361

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, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA63977, QCA9886, QCM6125, QCN7605, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM81- 181120/747

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM81- 181120/748

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

N/A02-Nov-204.6IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA5390, QCS405, QCS605, QM215, QRS165, Rennell, SA4155P, Sapan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM470, SDM429, SDM429W, SDM429, SDM430, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130https://w www.qualco mm.com/c ompany/p roduct- Snapdragon Mobile, Snapdragon Mobile, Snapdragon, SNR3150, SSM3155P, Saipan, SDA660, SDM630, SDM640, SDM640, SDM630, SDM640, SDM640, SDM640, SDM710, SM6150, SM150, SM8250, SXR1130, SXR2130 CVE UP : CVE-2020-111640-QUA-SM81- 181120/749<	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A02-Nov-204.6u'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, mm.com/c Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, SM8909W, MSM8917, Ulletins/oct tober- QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR21300-QUA-SM81- O-QUA-SM81- 181120/749				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,		
N/A02-Nov-204.6call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin02-Nov-204.6Call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8909W, MSM8917, Ulletins/oc tober- 2020- bulletin0-QUA-SM81- 181120/749 ulletins/oc 				CVE ID : CVE-2020-11162		
	N/A	02-Nov-20	4.6	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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-
Use After 02-Nov-20 4.4 u'Two threads running https://w 0-QUA-SM81-	Use After	02-Nov-20	4.4	u'Two threads running	https://w	0-0UA-SM81-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Wearables, Snapdragon Wired	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM81- 181120/751

0-1

1-2

2-3

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, 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, SDM632, SDM636, SDM660, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM81- 181120/752

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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_fir	mware				
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, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/753

0-1

1-2

2-3

4-5

5-6

6-7

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		
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-3670 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 Nobile, 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, SDM650, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/754

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/756

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/757

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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, 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_fir	mware				
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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/758

0-1

1-2

2-3

4-5

5-6

6-7

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/759

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/760

0-1

1-2

2-3

4-5

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial 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, QCA6390, QCA6574AU, QCA6377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS404, QCS405, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/761

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, Snapdragon Nobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 ww.qualco	0-QUA-MDM9- 181120/763

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, 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, SM6150, SM7150, SM8150, SM8250, SXR2130 	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
			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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/764

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130		
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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MDM9- 181120/765

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	CVE ID : CVE-2020-11174 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 Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8074, MDM9150, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/766
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

378

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_fir	mware				
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, MDM9205, MDM9206, MDM9640, MDM9645, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/767

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, 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, SDM630, SDM20, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p	O-QUA-MDM9- 181120/769

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

			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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, Sicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, Sicobar, QCA6174A, QCA6390, QCA6574AU, Sicobar, QCA6174A, Sicobar, Sicoba Sicobar, Sicoba Sicobar, Sicoba Sicobar, Sicoba Sicobar, Sicobar, Sicoba Sicobar, Sicobar, Sicoba Sicobar, Sicobar, Sicoba Sicobar, Sicobar, S	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 process due to lack of check	https://w ww.qualco mm.com/c	O-QUA-MDM9- 181120/770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM950, MSM8905, MSM8917, 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, SDM450, SM8250, SXR1130, SXR2130	ompany/p roduct- security/b ulletins/oc 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-QUA-MDM9- 181120/771

382

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, 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	cve iD : cve-2020-11157u'Array index underflowissue in adsp driver due toimproper check of channel idbefore used as array index.'in Snapdragon Auto,Snapdragon Compute,Snapdragon Connectivity,Snapdragon Consumer IOT,Snapdragon Mobile,Snapdragon Wearables,Snapdragon WiredInfrastructure andNetworking in Agatti,APQ8009, APQ8017,APQ8053, APQ8096AU,APQ8074, Kamorta,MDM9607, MDM9640,MDM9650, MSM8905,MSM8909W, MSM8953,MSM8906AU, QCA6390,QCA9531, QCM2150,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/772

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Buffer Copy without (Pcking Size of Input (Classic Buffer Overflow')02-Nov-2010QCS404, QCS405, QCS605, SA415M, SA615PS, SA615DS, SA415PS, Sapan, SC81800X, SDM630, SDM630, SDM630, SDM632, SDM636, SDM640, SDM632, SDM636, SDM640, SDM632, SDM636, SDM640, SDM632, SDM249, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR130Networking in 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 Muto, Snapdragon Mobile, Snapdragon Mobile, Snapdr	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Oor)02-Nov-2010 <td></td> <td></td> <td></td> <td>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</td> <td></td> <td></td>				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		
	without Checking Size of Input ('Classic Buffer	02-Nov-20	10	happen by sending acarefully crafted POST querywhen Device configuration isaccessed from a tetheredclient through webserverdue to lack of array boundcheck.' in Snapdragon Auto,Snapdragon Compute,Snapdragon Nobile,Snapdragon Nobile,Snapdragon WiredInfrastructure andNetworking in APQ8009,APQ8017, APQ8053,APQ8074, MDM9150,IDM9206, MDM9207C,MDM9607, MDM9640,MDM9650, MSM8905,MSM8906AU, QCA6574AU,QCS405, QCS610, QRB5165,SDM429, SDM429W,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	÷

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM845, SDX20, SDX24, SDX55, SM8250		
			CVE ID : CVE-2020-3657		
mdm9655_fii	mware				
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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM630, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/774

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
msm8996au_	firmware			1	
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, MDM9205, MDM9206, MDM9640, MDM9645, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8953, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/775
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow can happen as part of SIP message packet processing	https://w ww.qualco mm.com/c	0-QUA-MSM8- 181120/776

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	ompany/p roduct- security/b 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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MSM8- 181120/777

0-1

1-2

2-3

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 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 Witel Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM896AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-MSM8- 181120/779

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SOK6125, 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	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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-QUA-MSM8- 181120/780

0-1

1-2

2-3

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 Music, 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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/781

0-1

1-2

2-3

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		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	CVE ID : CVE-2020-3654 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 Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/782

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_fir	mware				
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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/783

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_fir	mware				
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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/784

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 Nobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/785
mdm9635m_f	firmware				
Out-of-	02-Nov-20	6.4	u'Potential out of bounds read while processing	https://w ww.qualco	O-QUA-MDM9-
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 394	6-7 7-8	8-9 9-10

bounds Read downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9635M, MDM9650, MDM9655, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM420, SDM630, SDM632, SDM20, SDX24, SDX55,	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 10T, Snapdragon Industrial 10T, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9645, MDM9655, MSM8909W, MSM8905, MSM8909W, MSM8917, MSM8940, MSM89973, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA45, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM670, SDM710, SDM845, SDM850,	bounds Read			downlink NAS transport	mm.com/c	181120/786
Element(IEI) NAS messagesecurity/bcontainer' in Snapdragonuiletins/ocAuto, Snapdragon Compute,tober-Snapdragon Consumer IOT,2020-Snapdragon Industrial IOT,bulletinSnapdragon Wearables inAgatti, APQ8053,APQ8096AU, APQ8098,Kamorta, MDM9150,MDM9205, MDM9206,MDM9205, MDM9206,MDM9625, MDM9640, MDM9645,MDM9650, MDM9655,MSM8905, MSM8909W,MSM8917, MSM8940,MSM8917, MSM8940,MSM8953, MSM8996AU,MSM8998, Nicobar,QCM2150, QCM6125,QCX2150, QCS610, QM215,Rennell, SA415M, Saipan,SC7180, SC8180X, SDA660,SDA845, SDM429,SDM429W, SDM439,SDM450, SDM632,SDM450, SDM630, SDM632,SDM636, SDM660, SDM670,SDM710, SDM845, SDM850,Image Additional Additiona				message due to improper	ompany/p	
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, MDM9206, MDM9645, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8995, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM670, SDM710, SDM845, SDM850,				length check of Information	roduct-	
Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM896AU, MSM8917, MSM896AU, MSM8977, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM450, SDM439, SDM450, SDM60, SDM				Element(IEI) NAS message	security/b	
Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9625, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM645, SDM650,				container' in Snapdragon	ulletins/oc	
Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9206, MDM96650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8997, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM670, SDM710, SDM845, SDM850,				Auto, Snapdragon Compute,	tober-	
Image: state in the state				Snapdragon Consumer IOT,	2020-	
Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9206, MDM9640, MDM9645, MDM9650, MDM9655, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM893, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA45, SDM429, SDM450, SDM630, SDM632, SDM450, SDM630, SDM670, SDM710, SDM845, SDM850,				Snapdragon Industrial IOT,	bulletin	
Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA45, SDM429, SDM450, SDM632, SDM450, SDM632, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				Snapdragon Mobile,		
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, SDA450, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				Snapdragon Wearables in		
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, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				Agatti, APQ8053,		
MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				APQ8096AU, APQ8098,		
MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM600, SDM670, SDM710, SDM845, SDM850,				Kamorta, MDM9150,		
MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, 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,				MDM9205, MDM9206,		
MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, 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,				MDM9625, MDM9635M,		
MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, 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,				MDM9640, MDM9645,		
MSM8917, MSM8940, MSM8953, MSM8996AU, 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,				MDM9650, MDM9655,		
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,				MSM8905, MSM8909W,		
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,				MSM8917, MSM8940,		
QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				MSM8953, MSM8996AU,		
QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				MSM8998, Nicobar,		
Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				e , e ,		
SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				QCS605, QCS610, QM215,		
SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				Rennell, SA415M, Saipan,		
SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,						
SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				SDA845, SDM429,		
SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,						
SDM710, SDM845, SDM850,				SDM450, SDM630, SDM632,		
				SDM636, SDM660, SDM670,		
SDX20, SDX24, SDX55,				SDM710, SDM845, SDM850,		
SM6150, SM7150, SM8150,						
SXR1130				SXR1130		
CVE ID : CVE-2020-3670				CVE ID : CVE-2020-3670		
qca9531_firmware	qca9531_firm	ware				
u'Use after free while https://w				u'Use after free while	https://w	
Use After installing new security rule ww.qualco 0-QUA-QCA9-	Use After			installing new security rule		0-0114-0649-
Free 02-Nov-20 4.6 in ipcrtr as old one is deleted mm.com/c 181120/787		02-Nov-20	4.6	in ipcrtr as old one is deleted	-	
and this rule could still be in ompany/p	1100			-	-	101120/707
				use for checking security	roduct-	

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	security/b ulletins/oc 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 Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA9- 181120/788

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Wired Infrastructure and	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA9- 181120/790

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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, 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_firm	iware				
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 Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA9- 181120/791

0-1

1-2

2-3

4-5

5-6

6-7

3-4

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6125, QCN7605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
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 Wearables in APQ8053, APQ8076,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA9- 181120/792
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

399

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_firm	iware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA9- 181120/793
sdm429_firm	ware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM4- 181120/794

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM4- 181120/795

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 Overfow 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 Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/796
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-1 0

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 Nobile, Snapdragon Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/797

0-1

1-2

2-3

4-5

5-6

6-7 7-8

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Industrial IOT, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/798
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	CVE ID : CVE-2020-11157 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 Wearables, Snapdragon Wired Infrastructure and	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM4- 181120/799

0-1

1-2

2-3

4-5

5-6

6-7

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		
Use After Free	02-Nov-20	4.4	CVE ID : CVE-2020-11162 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/800

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/801

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/802
			u'Remote code execution can	https://w	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-SDM4- 181120/803

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wiered 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, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM630, SDM845, SDX20, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	bulletin	
sdm632_firm	ware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/804

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/805

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/806

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Consumer IOT, Snapdragon Mobile, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/807
CVSS Scoring Sca	le 0-1	1-2	2-3 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/809

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/810

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, 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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/811
CVSS Scoring Scal	e 0-1	1-2	2-3 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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/812
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://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-SDM6- 181120/813
Buffer Overflow')			client through webserver due to lack of array bound	security/b ulletins/oc	

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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, 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_fir	mware			<u> </u>	
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/814

0-1

1-2

2-3

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, 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, SDM450, SDM630, SDM632, SDM450, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MSM8- 181120/815

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/816

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

					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 Wieta 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/817

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/819

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

			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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/820

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/821
msm8937_fir	mware				
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://w ww.qualco mm.com/c ompany/p	O-QUA-MSM8- 181120/822
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM636, SDM660, SDM670, SDM636, SDM660, SDM670, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	roduct- security/b ulletins/oc 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	https://w ww.qualco mm.com/c ompany/p roduct-	0-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							

423

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 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/b ulletins/oc tober- 2020- bulletin	
msm8940_fir	mware				
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, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/824

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/825

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 Overfow 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 Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/826
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Industrial IOT, Snapdragon Nobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/828

0-1

1-2

2-3

4-5

5-6

6-7

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/829

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130		
			CVE ID : CVE-2020-3654		
sdm450_firm	ware				
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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/830

0-1

1-2

2-3

4-5

5-6

6-7 7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Consumer IOT, 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, SDM420, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/831
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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE-	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/832

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM4- 181120/833

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, SDM55, 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 Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM4- 181120/834

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Buffer Copy without (Classic Buffer Overflow')02-Nov-204.6MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632https://wBuffer Copy without (Classic Buffer Overflow')u'Possible buffer overflow in MHI driver due to lack of input parameter validation of BOT events received from MHI device side' in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Weired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ8074, Kamorta, QCA6390, QCM2150, QCX5404, QCS405, QCS605, QM215, QRB165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Sah15D, SM8150, SM429, SDM429, SDM429, SDM429, SDM429, SDM439, SDM439, SDM430, SDM632, SDM439, SDM430, SDM632, SDM110, SDM435, SDM510, SCM210, SM220, SNR211300-QUA-SDM4- I81120/835N/A02-Nov-204.6u'Third-party app may alsohttps://w0-QUA-SDM4-	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')02-Nov-204.6u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, 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, SA6155P, SA8155P, Sahato, SDM439, SDM450, SDM632, SDM439, SDM450, SDM632, SDM419, SDM450, SM8150, SM8250, SXR2130https://w ww.qualco mm.com/c onpany/p roduct- tober- 2020- bulletin0.40APAPAPAP0.50A.66APAPAP0.60APAPAPAP0.70APAPAPAP0.71MSM8953, Nicobar, QCA64390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Sahato, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130O-QUA-SDM4-				MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439,		
Buffer Copy without Checking Sure of Input (Classic Buffer Overflow')02-Nov-204.6MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Compute, 				CVE ID : CVE-2020-11157		
N/A 02-Nov-20 4.6 u'Third-party app may also https://w 0-QUA-SDM4-	without Checking Size of Input ('Classic Buffer	02-Nov-20	4.6	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 Wieta Snapdragon Wieed 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, SM6150, SM7150, SM8150, SM8250, SXR2130	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-
	N/A	02-Nov-20	4.6	u'Third-party app may also	https://w	O-QUA-SDM4-

0-1

1-2

2-3

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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM4- 181120/837

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
iware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SM82- 181120/838
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	0-QUA-SM82- 181120/839
	02-Nov-20	02-Nov-20 4.6 0.1 1.0 0.2 1.0 0.1 1.0 0.1 1.0 0.1 1.0	O2-Nov-204.6Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM600, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130WareUUA n'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 Connectivity, Snapdragon Connectivity, Snapdragon Consumer 10T, Snapdragon Industrial I0T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR213002-Nov-2010u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to	02-Nov-20Nicobar, QCA6390, QCA6574AU, QCM2150, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM450, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654ware02-Nov-204.6u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon SoxR2130 CVE ID : CVE-2020-3638https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 202-Nov-2002-Nov-2010u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check tohttps://w ww.qualco mm.com/c ompany/p

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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM82- 181120/840

436

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 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, SDM670, SDM710, SM8450, SM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM82- 181120/841

0-1

2-3

1-2

4-5

5-6

7-8

6-7

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	0-QUA-SM82- 181120/844

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
			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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM82- 181120/845
CVSS Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Out-of- bounds02-Nov-204.6QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SCB180X, SDA845, SDM60, SDM670, SDM710, SDM845, SDM850, SDX20, SWR150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704Out-of- boundsu'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 Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Vice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Birra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9150, MSM8905, MSM8917, MSM8953, Nicobar, QCA5030, QCA9531, QCX2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA4159F, SA8155P, Saipan, SCB180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660,https://w wure0-QUA-SM82- 181120/846 uiletin	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- boundsAppen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Conpute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Noice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Security, PloSo18, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6330, QCA9531, QCX15150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415SP, Saipan, SA615SP, SA815SP, Saipan, SA615SP, SA815SP				QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
	bounds	02-Nov-20	4.6	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 Wied Snapdragon Wied 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	÷

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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SM82- 181120/847
			CVE ID : CVE-2020-11141		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM82- 181120/848

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID: CVE-2020-11162 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM82- 181120/849
N/A	02-Nov-20	4.6	u'Third-party app may also	https://w	O-QUA-SM82- 181120/850
N/A CVSS Scoring Scal		4.6 1-2	a minu-party app may alsocall the broadcasts in2-33-4442	6-7 7-8	181120/850 8-9 9-10

442

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/c ompany/p roduct- security/b 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 Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SM82- 181120/851

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, 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, SDM429W, SDM630,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM82- 181120/852
CVSS Scoring Sca	le 0-1	1-2	2-3 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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-SM82- 181120/854

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, SSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	security/b ulletins/oc tober- 2020- bulletin	
sxr2130_firm	ware			I	
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR2- 181120/855

0-1

1-2

2-3

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR2- 181120/856
N/A	02-Nov-20	4.6	u'QSEE reads the access	https://w	0-QUA-SXR2-

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

in Snapdragon Auto, roduct- Snapdragon Compute, security/b Snapdragon Connectivity, ulletins/oc Snapdragon Consumer IOT, tober-	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A 02-Nov-20 7.2 configuration, the modem ww.qualco crypto engine can potentially mm.com/c compromise the hypervisor' ompany/p in Snapdragon Auto, roduct- Snapdragon Connectivity, ulletins/oc Snapdragon Consumer IOT, tober-				SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, 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, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM630, SDM636, SM7150, SM8150, SM8250, SXR1130, SXR2130	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	181120/857
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	N/A	02-Nov-20	7.2	configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	•
	CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

448

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 Comsumer 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b	0-QUA-SXR2- 181120/860

0-1

1-2

2-3

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR2- 181120/862

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6125, 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 Wired	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR2- 181120/863

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, 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 Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR2- 181120/864

0-1

1-2

2-3

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	0-QUA-SXR2- 181120/866

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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	ompany/p roduct- security/b 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 Industrial IOT, Snapdragon Woile, Snapdragon Woile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR2- 181120/867

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR2- 181120/868

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firm	iware			<u> </u>	
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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA61- 181120/869

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA61- 181120/870
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,	https://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-SA61- 181120/871

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & 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	security/b ulletins/oc tober- 2020- bulletin	
			CVE ID : CVE-2020-3690		
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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA61- 181120/872

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p	0-QUA-SA61- 181120/874

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	roduct- security/b 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, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA61- 181120/875

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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		
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-11162 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	0-QUA-SA61- 181120/877

0-1

1-2

2-3

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 Mobile, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA61- 181120/878

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA61- 181120/879
Improper	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://w ww.qualco	0-QUA-SA61- 181120/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			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, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
sc8180x_firm	ware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC81- 181120/881

0-1

1-2

2-3

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, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
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 Wired Infrastructure and	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SC81- 181120/882

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SC81- 181120/884

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	CVE ID : CVE-2020-11154 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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC81- 181120/886

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')02-Nov-204.6Snapdragon Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250https://w ww.qualco of EOT events received from MHI device side' in Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, QCA6390, QCM2150, QCS404, QCS405, QCS405, QM215, QRB5165, Rennell, SA415SP, Sah15SP, Sah15SP, SAB15SP, Satism, SC8180X, SDM429, SDM429, SDM429, SDM429, SDM429, SDM429, SDM429, SDM450, SDM632,out out company/p roduct- security/b ulletin	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input (Classic Buffer Overflow')02-Nov-204.6u'Possible buffer overflow in MHI driver due to lack of input parameter validation of FOT events received from MHI device side' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wierd Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, Overflow')https://w ww.qualco ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin0-QUA-SC81- 181120/887				Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55,		
Buffer Copy without Checking Size of Input Overflow')02-Nov-204.6MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, 				CVE ID : CVE-2020-11156		
SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	without Checking Size of Input ('Classic Buffer	02-Nov-20	4.6	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 Wieta Snapdragon Wieed 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, SM6150, SM7150, SM8150, SM8250, SXR2130	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•
Integer 02-Nov-20 6.4 u'Buffer over-read while https://w 0-QUA-SC81-	Integer	02-Nov-20	6.4	u'Buffer over-read while	https://w	0-QUA-SC81-

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC81- 181120/889

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, 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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC81- 181120/890
CVSS Scoring Scal	e 0-1	1-2	2-3 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Comsumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC81- 181120/892

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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, 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 u'Potential out of bounds		
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, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC81- 181120/893

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

N/A02-Nov-204.6Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM430, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130https://w www.uakionumber of the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Vired IH76018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9206, SM80905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS6050, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Sapan, SC7180, SC8180X, SDA660, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
 N/A 02-Nov-20 4.6 N/A 02-Nov-20 4.6 MC <li< td=""><td></td><td></td><td></td><td>SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</td><td></td><td></td></li<>				SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130		
	N/A	02-Nov-20	4.6	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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC81- 181120/896

0-1

1-2

2-3

4-5

5-6

6-7

8-9

9-10

Out-of-bounds Read 02-Nov-20 7.5 7.5 7.5 7.5 7.5 7.5 7.5 8 02-Nov-20 7.5 7.5 8 02-Nov-20 7.5 7.5 8 02-Nov-20 7.5 7.5 0 02-Nov-20 7.5 7.5 0 02-Nov-20 7.5 0 02-Nov-20 7.5 0 02-Nov-20 0 02-Nov-20 0 <th>Weakness</th> <th>Publish Date</th> <th>CVSS</th> <th>Description & CVE ID</th> <th>Patch</th> <th>NCIIPC ID</th>	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read02-Nov-207.57.57.5Image: Constraint of the constraint				Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,		
Out-of- bounds Read02-Nov-207.5F.5Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link 				CVE ID : CVE-2020-3692		
Snapdragon Intaceriar 101)tober- 2020- bulletinSnapdragon 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,tober- 2020- bulletin		02-Nov-20	7.5	Bluetooth peripheralfirmware due to lack ofcheck for invalid opcode andlength of opcode receivedfrom central device(ThisCVE is equivalent to LinkLayer Length Overfow issue(CVE-2019-16336,CVE-2019-17519) and SilentLength Overflow issue(CVE-2019-17518) mentioned insweyntooth paper)' inSnapdragon Compute,Snapdragon Connectivity,Snapdragon ConsumerElectronics Connectivity,Snapdragon Industrial IOT,Snapdragon Industrial IOT,Snapdragon IoT, SnapdragonMobile, Snapdragon Voice &Music in APQ8053,APQ8076, AR9344, Bitra,Kamorta, MDM9206,MDM9207C, MDM9607,MSM8905, MSM8917,MSM8937, MSM8940,MSM8953, Nicobar,QCA6174A, QCA9377,QCM2150, QCM6125,QCS610, QM215, Rennell,SC8180X, SDM429, SDM439,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS404, QCS405, QCS605, QCS404, QCS405, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SC81- 181120/898
CVSS Scoring Sca	le 0-1	1-2	2-3 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_firm	ware				
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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, SM88917, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM8- 181120/899

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c	0-QUA-SDM8- 181120/901

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

		CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, 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, SDM650, SM7150, SM8150, SM8250, SXR1130, SXR2130	ompany/p roduct- security/b ulletins/oc tober- 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 VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM8- 181120/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, 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_firr	nware				
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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCM2- 181120/903

0-1

1-2

2-3

4-5

5-6

6-7

3-4

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8905, 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 Industrial IOT, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-QCM2- 181120/904

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, 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, SM6150, SM7150, SM8150, SM6150, SM7150, SM8150, SM8250, SXR2130 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b	O-QUA-QCM2- 181120/906

0-1

1-2

2-3

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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCM2- 181120/907

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCM2- 181120/908

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCM2- 181120/909
Improper	02-Nov-20	10	u'Buffer overflow can	https://w	0-QUA-QCM2-
Validation of			happen as part of SIP	ww.qualco	181120/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	mm.com/c ompany/p roduct- security/b 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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCM2- 181120/911

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Overfow issue	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-QUA-QCM2- 181120/913

0-1

1-2

2-3

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 Industrial 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	2020- bulletin	
advEE former			CVE ID : CVE-2020-3703		
sdx55_firmwa 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	0-QUA-SDX5- 181120/914

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX5- 181120/915

0-1

1-2

2-3

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		
Out-of- bounds Write	02-Nov-20	10	CVE ID : CVE-2020-11141 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 Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDX5- 181120/917

0-1

1-2

2-3

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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	O-QUA-SDX5- 181120/919

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDX5- 181120/920

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX5- 181120/922

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM600, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11173 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 Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Wearables, Snapdragon Wired https://w				MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130		
Improper Infrastructure and roduct- 0-QUA-SDX5 Validation of 02-Nov-20 4.6 Networking in Agetti		02-Nov-20	4.6	 issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, 	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-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-	CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

494

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX5- 181120/925

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX5- 181120/926

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

N/A02-Nov-204.6MSM8953, MSM8996AU, MSM8998, Nicobar, QCK2150, QCK6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM50, SDM50, SDM630, SDM632, SDM50, SDM50, SDM50, SDM20, SDM455, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130https://w www.qualco mm.com/c mmany/p roduct- sapdragon Mobile, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Mobile, <br< th=""><th>Weakness</th><th>Publish Date</th><th>CVSS</th><th>Description & CVE ID</th><th>Patch</th><th>NCIIPC ID</th></br<>	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Image: constraint of the series of the ser				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		
5701551, Saipail, 507100,	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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-

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 Industrial IOT, Snapdragon Woice & 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, SDM650, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDX5- 181120/928
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	CVE ID : CVE-2020-3690 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	O-QUA-SDX5- 181120/929

0-1

1-2

2-3

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDX5- 181120/930

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firmw	vare				
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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in AR9344	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE-	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-AR93- 181120/932

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-AR93- 181120/933
	02-Nov-20	02-Nov-20 7.8	02-Nov-207.8sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR113002-Nov-207.8u'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	02-Nov-207.8sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Notice & 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, SDM50, SXR113002-Nov-207.8u'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)' inhttps://w wulletim

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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SXR1130, SXR2130		
agatti_firmwa	ire				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	O-QUA-AGAT- 181120/934

0-1

1-2

2-3

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	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 Wired	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-AGAT- 181120/935

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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		
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-11162 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-AGAT- 181120/936

0-1

1-2

2-3

4-5

5-6

6-7

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 Wiced 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-AGAT- 181120/937
			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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-AGAT- 181120/938

0-1

1-2

2-3

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, APQ8017, APQ8053, APQ8096AU, APQ8053, APQ8096AU, APQ8053, APQ8096AU, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM632, SDM636, SDM429, SDM632, SDM636, SDM660, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-AGAT- 181120/939

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p	0-QUA-AGAT- 181120/941

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, 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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-AGAT- 181120/942

0-1

1-2

2-3

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-AGAT- 181120/944

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and applies them without validation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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	security/b ulletins/oc tober- 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-AGAT- 181120/945

0-1

1-2

2-3

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		
			u'Possible buffer overflow		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-AGAT- 181120/946
			CVE ID : CVE-2020-3692		
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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-AGAT- 181120/947

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
			CVE ID : CVE-2020-3704		
qrb5165_firm	iware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	0-QUA-QRB5- 181120/948

0-1

1-2

2-3

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(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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, 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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SOM6125, QCN7605, 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	happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto,	ww.qualco mm.com/c ompany/p roduct- security/b	O-QUA-QRB5- 181120/949

0-1

1-2

2-3

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, Snapdragon Wearables, 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, SDM450, SDM632, SDM660, SDM450, SM8250, SXR1130, SXR2130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QRB5- 181120/950

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-QRB5- 181120/951

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firm	ware			L	
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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p	0-QUA-QCN7- 181120/953
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

('Classic Buffer Overflow')copying into it.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Vired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCV7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55https://w www.qualco mm.compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCV7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55https://w www.qualco mm.com/c ompany/p roduct- scurty/b Ill 20/954o-QUA-QCN7- 181120/954Integer Overflow or Wraparound02-Nov-206.46.4Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Electronics Snapdragon Mobile, Snapdragon Consumer Electronics Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8093, QCA6390, QCV7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55https://w electronics Connectivity, Snapdragon Wired Infrastructure and Networking in APQ809, APQ8053, QCA6390, QCV7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55o-QUA-QCN7- illetin	Buffer Overflow')IseaSnapdragon Auto, Snapdragon Compute, Snapdragon Consumersecurity/b ulletins/oc tober- 2020- bulletinOverflow')Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55Image 1000000000000000000000000000000000000	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer 02-Nov-20 04.4 u'Buffer over-read while Overflow check' in 5napdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Overflow or 02-Nov-20 6.4 Snapdragon Consumer <td>Integer 02-Nov-200 6.4 u'Buffer over-read while Nutber overflow check' in Naparagon Auto, Snapdragon Auto, Nutber overflow check' in Nutber overflow check' in Snapdragon Compute, Snapdragon Connectivity, Nw.qualco Nw.qualco Snapdragon Consumer mm.com/ce Snapdragon Consumer Mw.qualco Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Security/be Naparagon Mobile, Snapdragon Mobile, Sunapdragon Mobile, Security/be Infrastructure and 2020- 181120/954 Networking in APQ8009, APQ8053, QCA6390, Uletinn QCN7605, QCN7606, SA4155N, SA515SN, SA6155P, SA8155P, SC8180X, SDX55</td> <td>Buffer</td> <td></td> <td></td> <td>Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P,</td> <td>security/b ulletins/oc tober- 2020-</td> <td></td>	Integer 02-Nov-200 6.4 u'Buffer over-read while Nutber overflow check' in Naparagon Auto, Snapdragon Auto, Nutber overflow check' in Nutber overflow check' in Snapdragon Compute, Snapdragon Connectivity, Nw.qualco Nw.qualco Snapdragon Consumer mm.com/ce Snapdragon Consumer Mw.qualco Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Security/be Naparagon Mobile, Snapdragon Mobile, Sunapdragon Mobile, Security/be Infrastructure and 2020- 181120/954 Networking in APQ8009, APQ8053, QCA6390, Uletinn QCN7605, QCN7606, SA4155N, SA515SN, SA6155P, SA8155P, SC8180X, SDX55	Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P,	security/b ulletins/oc tober- 2020-	
Integer Overflow or Wraparound02-Nov-2006.46.4processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumerhttps://w ww.qualco mm.com/c Ompany/p roduct- Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX550-QUA-QCN7- 0-QUA-QCN7- 181120/954 Ulletins/oct bulletin	Integer Overflow or Wraparound02-Nov-206.4For the second				CVE ID : CVE-2020-11155		
	sda660_nrmware	Overflow or Wraparound		6.4	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 Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, 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, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDA6- 181120/955
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://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-SDA6- 181120/956
CVSS Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

N/A 02-Nov-20 4.6 validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consuter 10T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8906AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QC8605, QM215, Rennel, SA6155P, Salis5P, Saipan, SDA660, SDM429, SDM420, SDM630, SDM632, SDM450, SDM630, SDM632, SDM36, SDM630, SDM632, SDM36, SDM650, SDM650, SM7110, SM8150, SM8250, SXR1130, SXR2130 validate the index length' in m.com/c ompany/p roduct security/b ultetin/s Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Snap	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/AO2-Nov-20A.6U'QSEE reads the accessInfrastructure andInfrastructure andN/A02-Nov-204.6Infrastructure andInfrastructure andInfrastructure andInfrastructure and				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	ulletins/oc tober- 2020-	
	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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

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 u'Third-party app may also		
N/A	02-Nov-20	4.6	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDA6- 181120/958

0-1

1-2

2-3

4-5

5-6

6-7

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDA6- 181120/959
Improper Validation of	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://w ww.qualco	0-QUA-SDA6- 181120/960
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	mm.com/c ompany/p roduct- security/b 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDA6- 181120/961

0-1

1-2

2-3

4-5

5-6

6-7

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, 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_firm	ware				
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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/962

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
Improper Input Validation	02-Nov-20	5	CVE ID : CVE-2020-11125 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 Industrial IOT, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/963

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	0-QUA-SDM4- 181120/965

0-1

1-2

2-3

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, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/966

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, 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 Consumer IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/967

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Overfow 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 Industrial IOT, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM4- 181120/968
CVSS Scoring Sca	le 0-1	1-2	2-3 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_firm	ware				
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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9640, MDM9645, MDM9650, MDM9635M, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/969

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	O-QUA-SDM6- 181120/971

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Auto, Snapdragon Compute, Snapdragon Connectivity,tober- 2020- bulletinSnapdragon 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, MDM9650, MSM8905tober- 2020- bulletin			CVSS	Publish Date	Weakness
MSM3030, MSM0303, 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	Connectivity, 2020- Consumer IOT, bulletin Industrial IOT, bulletin Mobile,	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, 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			
Out-of- bounds Read02-Nov-207.5Image: Comparison of the	ripheral https://w alid opcode and ww.qualco ode received mm.com/c device(This ompany/p alent to Link roduct- 0-QUA-SDM6- 1 Overfow issue security/b 6336,CVE- ulletins/oc and Silent tober- low issue(CVE- 2020-) mentioned in bulletin paper)' in until the security of the	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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in	7.5	02-Nov-20	

531

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/973

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 Woice & 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, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/974

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b	O-QUA-SDM6- 181120/976

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	ulletins/oc tober- 2020- bulletin	
sdm660_firm	ware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/977

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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,MSM8917, MSM8940,MSM8953, MSM8996AU,MSM8953, MSM8996AU,MSM898, Nicobar,QCM2150, QCM6125,QCS605, QCS610, QM215,Rennell, SA415M, Saipan,SC7180, SC8180X, SDA660,SDA459, SDM429,SDM429W, SDM439,SDM450, SDM630, SDM632,SDM636, SDM660, SDM670,SDX20, SDX24, SDX55,SM6150, SM7150, SM8150,SXR1130CVE 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/978

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

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, SXR2130CVE ID : CVE-2020-3673u'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 Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Computing	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
u'QSEE reads the accesspermission policy for theSMEM TOC partition fromthe SMEM TOC contentspopulated by XBL Loaderand applies them withoutvalidation' in SnapdragonAuto, Snapdragon Compute,				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		
SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Auto, Snapdragon Compute,				u'QSEE reads the access		
Snapdragon Consumer IOT,https://wSnapdragon Industrial IOT,ww.qualcoSnapdragon Mobile,mm.com/cSnapdragon Voice & Music,ompany/p	N/A	02-Nov-20	4.6	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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-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	CVSS Scoring Sca	ale <u>0-1</u>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

537

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 Overfow 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 Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/980
CVSS Scoring Sca	le 0-1	1-2	2-3 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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial 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, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/981
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Nobile, Snapdragon Wierel 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, SDM420W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/982

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDM6- 181120/984

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Nobile, Snapdragon Wied Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8906AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/985

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/986

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Nobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDM6- 181120/987
mdm9150_fir	mware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b	0-QUA-MDM9- 181120/988

0-1

1-2

2-3

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, MDM9205, MDM9206, MDM9640, MDM9635M, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	ulletins/oc 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 Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MDM9- 181120/989

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MDM9- 181120/990

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9206, MDM9207C, MDM9607, MDM9640,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/991

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_fir	mware				
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, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/992

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS404, QCS405, Rennell,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/993
CVSS Scoring Scal	e 0-1	1-2	2-3 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	O-QUA-MDM9- 181120/995

0-1

1-2

2-3

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 Wiede Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MDM9- 181120/996

0-1

1-2

2-3

4-5

5-6

6-7

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, 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_f	irmware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MSM8- 181120/997

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130		
			CVE ID : CVE-2020-3670 u'Buffer overflow can		
Improper Validation of Array Index	02-Nov-20	10	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 Consumer IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/998

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 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 Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MSM8- 181120/1000

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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		
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-3696 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-MSM8- 181120/1002

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Music, 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, 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/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, Snapdragon Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-MSM8- 181120/1003

0-1

1-2

2-3

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 Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-MSM8- 181120/1004

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firmv	vare				
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, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1005

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

	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		
Improper Validation of Array Index	02-Nov-20	10	CVE ID : CVE-2020-3670 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1006
Buffer Copy	02-Nov-20	4.6	u'A buffer overflow could	https://w	0-QUA-QCS6-

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1008
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

560

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 Industrial IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1009
			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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1010

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-QCS6- 181120/1012

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from central device(This	security/b	
			CVE is equivalent to Link	ulletins/oc	
			Layer Length Overfow issue	tober-	
			(CVE-2019-16336,CVE-	2020-	
			2019-17519) and Silent	bulletin	
			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		
			u'While processing invalid	https://w	
1			connection request PDU	ww.qualco	
Improper	02 No 20	7.0	which is nonstandard	mm.com/c	0-QUA-QCS6-
Input Validation	02-Nov-20	7.8	(interval or timeout is 0)	ompany/p	181120/1013
Validation			from central device may lead	roduct-	
			peripheral system enter into	security/b	
			I I		

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Out-of- bounds 02-Nov-20 4.6 dead lock state.(This CVE is equivalent to InvalidConnectionRequest(C 2020- VE-2019-19193) mentioned bulletin in sweyntooth paper)' in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IDT, Snapdragon Mitted Infrastructure and Networking in Agatti, APQ8003, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM96650, MSK8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM640, SDM670, SDM710, SDM845, SDM650, SDX20, SXR1130, SXR2130 0-QUA-QCS6- mm.com/c organy/p rocess due to lack of check of channel id value received from MHI devices' in 0-QUA-QCS6- 81120/1014	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write02-Nov-204.6happen in MHI command process due to lack of check of channel id value received from MHI devices' inww.qualco mm.com/c ompany/p roduct-0-QUA-QCS6- 181120/1014				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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, 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	
	bounds	02-Nov-20	4.6	happen in MHI command process due to lack of check of channel id value received	ww.qualco mm.com/c ompany/p	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

564

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 Woice & 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/b 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	O-QUA-QCS6- 181120/1015

0-1

1-2

2-3

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1016

566

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 u'Array index underflow		
Improper Validation of Array Index	02-Nov-20	4.6	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 Nobile, Snapdragon Wieed Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1017

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1018
sdx20_firmwa	are				
			u'Potential out of bounds	https://w	
Out-of- bounds Read	02-Nov-20	6.4	read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute,	nttps://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-QUA-SDX2- 181120/1019

0-1

1-2

2-3

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, 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX2- 181120/1020

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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		
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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX2- 181120/1021

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Overfow 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX2- 181120/1023

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM636, SDM660, SDM670, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130		
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX2- 181120/1024

0-1

1-2

2-3

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDX2- 181120/1025

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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 Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX2- 181120/1026

0-1

1-2

2-3

4-5

5-6

6-7

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_firm	ware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b	O-QUA-SM71- 181120/1028

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index	02-Nov-20	10	CVE ID : CVE-2020-3670 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM71- 181120/1029

0-1

1-2

2-3

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, MSM8900, 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM71- 181120/1030

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p	O-QUA-SM71- 181120/1032

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	roduct- security/b 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM71- 181120/1033

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM71- 181120/1034

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 Industrial IOT, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM71- 181120/1035

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	CVE ID : CVE-2020-11125 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Noice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM71- 181120/1036

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM71- 181120/1037
			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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SM71- 181120/1038

0-1

1-2

2-3

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SM71- 181120/1039

0-1

1-2

2-3

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_firm	iware				
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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM630, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR1- 181120/1040

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR1- 181120/1041
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SXR1- 181120/1042

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c	O-QUA-SXR1- 181120/1044

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, 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	ompany/p roduct- security/b 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR1- 181120/1045

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Improper Input Validation 02-Nov-20 7.8 1 1 1 1 1 1 1 1 1 1 1 1 1	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation02-Nov-207.87.8u'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 Consumer Electronics Connectivity, Snapdragon Industrial 10T, Snapdragon IoT, Snapdragon Voice &https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletin0-QUA-SXR1- 181120/1046				Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, 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,		
Improper Input Validation02-Nov-207.87.8connection 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice &https://w ww.qualco omm.com/c o-QUA-SXR1- 181120/1046				CVE ID : CVE-2020-3703		
Music, Snapdragon Wired	Input	02-Nov-20	7.8	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 Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

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, 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 Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SXR1- 181120/1047

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR1- 181120/1048

0-1

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	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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SXR1- 181120/1049
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	https://w ww.qualco mm.com/c ompany/p roduct-	O-QUA-SXR1- 181120/1050

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, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	security/b ulletins/oc tober- 2020- bulletin	
sdy24 firmwa	aro				
sdx24_firmwa			u'Potential out of bounds		
Out-of- bounds Read	02-Nov-20	6.4	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX2- 181120/1051

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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, 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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SDX2- 181120/1052

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDX2- 181120/1053
Buffer Copy	02-Nov-20	10	u'Possible buffer overflow	https://w	0-QUA-SDX2-
Duner copy				110051// 1	o gon obne

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/1054
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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDX2- 181120/1055

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Overfow 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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDX2- 181120/1056

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Improper Input Validation02-Nov-207.8SM®150, SXR1130 CVE ID : CVE-2020-3703
Improper Input02-Nov-207.8u'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 Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Industrial I07, Snapdragon I07, Snapdragon Mired Infrastructure and Networking in Agati, APQ8009, APQ8017, APQ8009, APQ8017, APQ8009, APQ8017, APQ8009, APQ8017, APQ8009, APQ8017, APQ8009, APQ8017, APQ8009, APQ8017, APQ8009, APQ8017, APQ8009, APQ8017, APQ8037, QCA6374AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCS404, QCS405, QCS405, QCS405, QCS404, QCS405, SDX805, SDX845, SDM600, SDM670, SDM710, SDM845, SDM850, SDX20,0-QUA-SDX2- tele
Improper Input ValidationR.N.R.N.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 VF-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Consumer Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Snapdragon Consumer Dispatagon Consumer Snapdragon Consumer Mobile, Snapdragon Consumer Mobile, Snapdragon Nuto Snapdragon IoT, Snapdragon Mustrial IOT, Snapdragon IoT, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ809, APQ8017, APQ809, APQ8017, APQ809, APQ8017, APQ8050, SNB4956, SDN8040, Nicobar, QCA6174A, QCA6377, QCA9866, QCS610, QRB5165, Rennell, SA145M, SA515M, Sajpan, SC7180, SCB180X, SDN845, SDM60, SDM670, SDM20,https://w ww.qualco mm.com/c ompany/p roduct- scurity/b ultetins/cc tober- 2020- builetin

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 Nobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SDX2- 181120/1058
Buffer Copy	02-Nov-20	10	u'Remote code execution can	https://w	0-QUA-SDX2-
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 599	6-7 7-8	8-9 9-10

599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness without Checking Size of Input ('Classic Buffer Overflow')	Publish Date	CVSS	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 Nobile, 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	Patch ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	NCIIPC ID 181120/1059
			CVE ID : CVE-2020-3657		
rennell_firmv	vare			I	
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	O-QUA-RENN- 181120/1060

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-RENN- 181120/1061

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-RENN- 181120/1062

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-RENN- 181120/1063
			CVE ID : CVE-2020-11173 u'An Unaligned address or	https://w	
Incorrect Default Permissions	02-Nov-20	4.6	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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	O-QUA-RENN- 181120/1064

0-1

1-2

2-3

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-RENN- 181120/1065

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Out-of- bounds Read 02-Nov-20 6.4 02-Nov-20 6.4 02-Nov-20 6.4 02-Nov-20 0.4	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read02-Nov-206.4u'Potential out of bounds read while processing downlink NAS transport 				SXR1130, SXR2130		
Out-of- bounds Read02-Nov-206.4read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Scale, APQ8096AU, APQ8096AU, MDM9610, MDM9615, MDM9610, MDM9615, MDM9625, MDM9635, Scale, SDM610, SDM630, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM630, SDM632, SDM450, SDM630, SDM630, SDM630, SDM450, SDM630, SDM630, SDM630, SDM4510, SM150, SXR1130 CVE ID : CVE-2020-3670Lt				CVE ID : CVE-2020-3654		
Improper as a to U'Buffer overflow can https://w 0-0UA-RENN-		02-Nov-20	6.4	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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, SDM429, SDA450, SDM6125, 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-
Validation of 02-Nov-20 10 happen as part of SIP ww.qualco 181120/1067	Improper	02-Nov-20	10	u'Buffer overflow can	https://w	O-QUA-RENN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	mm.com/c ompany/p roduct- security/b ulletins/oc 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-RENN- 181120/1068

0-1

1-2

2-3

4-5

5-6

7-8

8-9

9-10

			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		
N/A	02-Nov-20	7.2	CVE ID : CVE-2020-3684 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 Industrial IOT, 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-RENN- 181120/1069

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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-RENN- 181120/1070
			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 Overfow 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 Consumer Electronics Connectivity,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-RENN- 181120/1071

0-1

1-2

2-3

4-5

5-6

6-7

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, 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon InT, Snapdragon	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-RENN- 181120/1072

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6125, 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		
sa415m_firm	ware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA41- 181120/1073

0-1

1-2

2-3

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, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SA41- 181120/1074

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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, SDM670, SDM710, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c	0-QUA-SA41- 181120/1076

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
Improper Input Validation	02-Nov-20	7.8	CVE ID : CVE-2020-3692 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA41- 181120/1077

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA41- 181120/1078

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA41- 181120/1079
			CVE ID : CVE-2020-11141 u'Buffer overflow while	https://w	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	O-QUA-SA41- 181120/1080

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p	0-QUA-SA41- 181120/1082

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Woile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250	roduct- security/b ulletins/oc tober- 2020- bulletin	
			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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA41- 181120/1083

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA41- 181120/1085

0-1

1-2

2-3

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, MSM8909W, MSM8953, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM632, SDM636, SDM660, SDM632, SDM636, SDM660, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130		
saipan_firmw	are				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SAIP- 181120/1086

0-1

1-2

2-3

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, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM632, SDM636, SDM660, SDM670, 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 Consumer IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SAIP- 181120/1087

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SAIP- 181120/1088

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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, SDM670, SDM710, SM8150, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SAIP- 181120/1090

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SAIP- 181120/1091
			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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SAIP- 181120/1092
Improper				https://	
Input Validation	02-Nov-20	7.8	u'While processing invalid connection request PDU which is nonstandard	https://w ww.qualco mm.com/c	0-QUA-SAIP- 181120/1093

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

624

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 Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Wieel Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM950, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDM450, SM8250, SXR1130, SXR2130	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/1094
			CVE ID : CVE-2020-11125		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	O-QUA-SAIP- 181120/1095

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SAIP- 181120/1096

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wiedarables, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c	0-QUA-SAIP- 181120/1098

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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, 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	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
			CVE ID : CVE-2020-11174 u'Buffer overflow occurs	https://w	
Improper Validation of Array Index	02-Nov-20	10	while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-QUA-SAIP- 181120/1099

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	2020- bulletin	
ipq6018_firm	ware				
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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-IPQ6- 181120/1100

0-1

1-2

2-3

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 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ6- 181120/1101

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, 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, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ6- 181120/1102
Buffer Copy without	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of	https://w ww.qualco	0-QUA-IPQ6- 181120/1103

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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, SM8250, SXR2130 CVE ID : CVE-2020-11162	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ6- 181120/1104

0-1

1-2

2-3

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	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 Wearables, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ6- 181120/1105
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ6- 181120/1106

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wired Infrastructure and Networking in APQ8009,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-IPQ6- 181120/1107

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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_firm	iware			1	
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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-KAMO- 181120/1108

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

			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	CVE ID : CVE-2020-11125u'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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-KAM0- 181120/1109

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-KAMO- 181120/1111

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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		
Improper Validation of Array Index	02-Nov-20	4.6	CVE ID : CVE-2020-11173 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8996AU, QCA6390,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-KAMO- 181120/1112

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	O-QUA-KAMO- 181120/1114

0-1

1-2

2-3

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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-KAMO- 181120/1115

0-1

1-2

2-3

4-5

5-6

7-8

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-KAMO- 181120/1116

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-KAMO- 181120/1118

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

			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 0	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 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, SDM670, SDM710, SM8450, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-KAMO- 181120/1119
Buffer Copy O without	02-Nov-20	10	u'Possible buffer overflow while updating output buffer	https://w ww.qualco	O-QUA-KAMO- 181120/1120

643

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	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
			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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-KAMO- 181120/1121

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-KAMO- 181120/1122

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firmwai	re			1	
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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-BITR- 181120/1123

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	CVE ID : CVE-2020-11125 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-BITR- 181120/1124

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-BITR- 181120/1126

0-1

1-2

2-3

4-5

5-6

6-7

3-4

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 Woice & 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, MSM8906AU, QCA6390,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-BITR- 181120/1127

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	O-QUA-BITR- 181120/1129

0-1

1-2

2-3

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, 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 Consumer IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-BITR- 181120/1130

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

N/A02-Nov-204.6UCA6390, QCA6574AU, QCM2150, QCS055, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM420, SDM430, SDM630, SDM632, SDM36, SDM630, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130https://w www.uakionumber of the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Industrial IOT, Snapdragon Onset IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Vired Infrastructure and NDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9206, SMSM9998, Nicobar, QCA6390, QCS404, QCS405, QCS6050, QCS605, QCS605, QCS404, QCS405, QCS6050, QCS404, QCS405, QCA6390, QCS404, QCS405, SDM630, SDM630, SDM640, SDM630, SDM640, SDM630, SDM640, SDM640, SDM630, SDM640, SDM640, SDM630, SDM640, SDM640, SDM630, SDM640, SDM640, SDM630, SDM640, SDM640, SDM640, SDM640, SDM630, SDM244,https://w W.Qualetin	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
 N/A 02-Nov-20 4.6 N/A 02-Nov-20 1.6 <l< td=""><td></td><td></td><td></td><td>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</td><td></td><td></td></l<>				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		
	N/A	02-Nov-20	4.6	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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-BITR- 181120/1133

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-BITR- 181120/1134
			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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-BITR- 181120/1135

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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 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://w ww.qualco	
Improper Input Validation	02-Nov-20	7.8	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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-BITR- 181120/1136
CVSS Scoring Scal	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

655

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, 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_firmw	vare				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1137

0-1

1-2

2-3

4-5

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	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, MDM9205, MDM9206, MDM9640, MDM9645, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c	0-QUA-QCS6- 181120/1139

0-1

1-2

4-5

5-6

6-7

7-8

8-9

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, SDM670, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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 Overfow issue	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-QUA-QCS6- 181120/1142

0-1

1-2

2-3

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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8937, MSM8940, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM630, SDM632, SDM450, SDM630, SDM630, SDM632, SDM450, SDM630, SDM630, SDM63	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-QCS6- 181120/1143

0-1

1-2

2-3

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 Wearables, Snapdragon Wired	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1145

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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		
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 Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCS6- 181120/1146

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firm	iware				
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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, 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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA81- 181120/1147

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA81- 181120/1148
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	0-QUA-SA81- 181120/1149
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

665

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	tober- 2020- bulletin	
			CVE ID : CVE-2020-3690		
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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA81- 181120/1150

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b	0-QUA-SA81- 181120/1152

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	ulletins/oc tober- 2020- bulletin	
			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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA81- 181120/1153

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-SA81- 181120/1155

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA81- 181120/1156

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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	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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA81- 181120/1157
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack	https://w ww.qualco mm.com/c	0-QUA-SA81- 181120/1158

0-1

1-2

2-3

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
sa515m_firm	ware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SA51- 181120/1159

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA51- 181120/1160

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SA51- 181120/1162

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6125, 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		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA51- 181120/1163

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-SA51- 181120/1164

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA51- 181120/1165
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	CVE ID : CVE-2020-11154 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA51- 181120/1166

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA51- 181120/1168

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9 **9-1**0

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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		
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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA51- 181120/1169

0-1

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA51- 181120/1170
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-SA51- 181120/1171

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8909W, MSM8953, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM632, SDM636, SDM660, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130		
mdm9645_fir	mware				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	O-QUA-MDM9- 181120/1172

0-1

1-2

2-3

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, 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_firm 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 Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA4- 181120/1173

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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_firm	ware				
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 Industrial IOT, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/1174
			CVE ID : CVE-2020-3638 u'Buffer overflow can	https://w	
Improper Validation of Array Index	02-Nov-20	10	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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/1175

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8900, 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/1176

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
			u'Due to an incorrect SMMU configuration, the modem		
N/A	02-Nov-20	7.2	crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/1177
Impropor			u'While processing invalid	https://w	
Improper Input Validation	02-Nov-20	7.8	connection request PDU which is nonstandard (interval or timeout is 0)	ww.qualco mm.com/c ompany/p	0-QUA-QCA6- 181120/1178

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Out-of- bounds02-Nov-204.6from central device may lead peripheral system enter into dead lock state. (This CVE is security/b ulletins/oc tober- 2020- bulletinroduct- security/b ulletins/oc tober- 2020- bulletinInvalidConnectionRequest(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Noice & Music, Snapdragon Voice & Music, Snapdragon, AR9344, Bitra, IPQ5018, Kamorta, MDM9650, MSM896AU, Nicobar, QCA6174A, QCA6390, QCA574AU, QCA63977, QCA9886, QCM5125, QCS605, QCS610, QRB5155, Rennell, SA15M, Saipan, SC7180, SC8180X, SDM845, SDM660, SDM670, SDM710, SDM845, SDM850, SDM20, SDM845, SDM850, SDM20, SDM310, SXR1130 CVE ID : CVE-2020-3704https://w ww.qualco mu.com/c0-QUA-QCA6- 181120/1179	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Nov-204.6 happen in MHI commandWw.qualco0-QUA-QLA6- 181120/1179				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 Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial 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, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS404, QCS405, QCS605, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM7150, SM8150, SM8250, SXR1130, SXR2130	security/b ulletins/oc tober- 2020-	
		02-Nov-20	4.6	happen in MHI command	ww.qualco	

Write			of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
			Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, 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	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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	0-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

687

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 Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	0-QUA-QCA6- 181120/1182

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-QCA6- 181120/1184

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250	security/b ulletins/oc tober- 2020- bulletin	
			CVE ID : CVE-2020-11156 u'Possible buffer overflow in		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/1185

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/1187

0-1

1-2

2-3

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/1188

0-1

1-2

4-5

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	0-QUA-QCA6- 181120/1189
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	https://w ww.qualco mm.com/c ompany/p roduct-	0-QUA-QCA6- 181120/1190

693

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	security/b ulletins/oc tober- 2020- bulletin	
			CVE ID : CVE-2020-3654		
ZTE	_				
zxa10_eodn_f	irmware				
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
	<u> </u>		Hardware	J	
CVSS Scoring Sca	ale 0-1	1-2	2-3 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	imomobile								
verve_connec	t_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.	N/A	H-IMO-VERV- 181120/1192				
			CVE ID : CVE-2020-27689						
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 Neutralizatio n 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				

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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		
Mitsubishiele	ectric			I	
melsec_iq-rj7	1eip91				
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 RD810PC96 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- 181120/1196

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 RD810PC96 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- 181120/1197
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	N/A	H-MIT-MELS- 181120/1198

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9 9-10

			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 RD810PC96 0PC 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 RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network	N/A	H-MIT-MELS- 181120/1199

698

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 RD810PC96 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

0-1

1-2

2-3

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 RD810PC96 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-rj7	1pn92			Γ	
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

0-1

1-2

2-3

4-5

5-6

6-7

3-4

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Module First 2 digits of serial number are '04' or before, and RD810PC96 0PC 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 RD810PC96 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
	02-Nov-20	5	NULL pointer dereferences	N/A	H-MIT-MELS-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Pointer Dereferencevulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (R/TEIP91 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 '04' or before, and RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before, and RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before, and RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before) a specially crafted packet.N/AH-MIT-MELS- 181120/1205N/A02-Nov-207.5Improper 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, RD12D91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RD21D205N/A	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A 02-Nov-20 7.5 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				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 RD810PC96 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.		181120/1204
	N/A	02-Nov-20	7.5	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	N/A	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10					6-7 7-8	

702

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 RD810PC96 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.		
Argument Injection or Modification	02-Nov-20	3.3	CVE ID : CVE-2020-5656 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 RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers	N/A	H-MIT-MELS- 181120/1206

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
			Resource Management		
Uncontrolled Resource Consumption	02-Nov-20	5	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 RD810PC96 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-rd8	81dl96				
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 Sca	le 0-1	1-2	2-3 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')			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 RD810PC96 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 RD810PC96 OPC	N/A	H-MIT-MELS- 181120/1209

0-1

1-2

2-3

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 RD810PC96 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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 RD810PC96 0PC 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.		
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	N/A	H-MIT-MELS- 181120/1212
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

707

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 RD810PC96 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		
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 RD810PC96 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	N/A	H-MIT-MELS- 181120/1213

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a specially crafted packet.		
			CVE ID : CVE-2020-5658		
melsec_iq-rd8	81mes96n			L	
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 RD810PC96 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	N/A	H-MIT-MELS- 181120/1215
			'02' or before, RJ71PN92 PROFINET IO Controller		

0-1

1-2

2-3

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 RD810PC96 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 RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a	N/A	H-MIT-MELS- 181120/1216

710

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 RD810PC96 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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 RD810PC96 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		
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,	N/A	H-MIT-MELS- 181120/1219
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

712

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 RD810PC96 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-rd	81opc96				
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 RD810PC96 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

0-1

1-2

2-3

4-5

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	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 RD810PC96 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- 181120/1221
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	N/A	H-MIT-MELS- 181120/1222

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

			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 RD810PC96 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 RD810PC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated	N/A	H-MIT-MELS- 181120/1223

715

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 RD810PC96 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

0-1

1-2

2-3

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 RD810PC96 0PC 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 Neutralizatio n 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://v ww.qual	H-()IIA-MI)M9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			downlink NAS transport	mm.com/c	181120/1227
			message due to improper	ompany/p	
			length check of Information	roduct-	
			Element(IEI) NAS message	security/b	
			container' in Snapdragon	ulletins/oc	
			Auto, Snapdragon Compute,	tober-	
			Snapdragon Consumer IOT,	2020-	
			Snapdragon Industrial IOT,	bulletin	
			Snapdragon Mobile,		
			Snapdragon Wearables in		
			Agatti, APQ8053, APQ8096AU, APQ8098,		
			Kamorta, MDM9150,		
			MDM9205, MDM9206,		
			MDM9203, MDM9200, MDM9625, MDM9635M,		
			MDM9623, 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		
			u'QSEE reads the access	https://w	
			permission policy for the	ww.qualco	
			SMEM TOC partition from	mm.com/c	H-QUA-MDM9-
N/A	02-Nov-20	4.6	the SMEM TOC contents	ompany/p	181120/1228
			populated by XBL Loader	roduct-	101120/1220
			and applies them without	security/b	
			validation' in Snapdragon	ulletins/oc	
		4.2			
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

718

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 Vired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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, SDM630, SDM636, 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 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 Wired Snapdragon Wired Infrastructure and	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1229

0-1

1-2

2-3

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8937, MSM8940,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1230

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Buffer Copy without (Cckair)02-Nov-201002-Nov-201002-Nov-201002-Nov-2010Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and INFrequence, Nager May Source, MD99050, MD89050, MD89050, MD89050, MD89206, MD89205, MD89050, MD89050, MD89206, MD89205, MD89050, MD89205, MD8953, MSM899050, MD89206, MD89205, MSM89050, MD89205, MD8953, MSM89050, MD89205, MD8429, SDM429W, SDM429, SDM429W, SDM630, SDM632, SDM636,H-QUA-MDM9- 10	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')02-Nov-2010happen 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Wearables, roduct- security/b ulletins/oc tober- 2020- bulletinH-QUA-MDM9- 181120/1231Buffer Overflow')02-Nov-2010Snapdragon Nobile, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064U, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9607, MDM9653, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, SDM429W,H-QUA-MDM9- istractional interval interval security/b ulletin				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		
	without Checking Size of Input ('Classic Buffer	02-Nov-20	10	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 Nobile, Snapdragon Wied 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM845, SDX20, SDX24, SDX55, SM8250		
			CVE ID : CVE-2020-3657		
mdm9607				I	
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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1232

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SM8250, SXR2130 CVE ID: CVE-2020-11162 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-MDM9- 181120/1234

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1235

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Compute, Snapdragon Industrial IOT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1236

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-3657 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1237

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1239

0-1

1-2

2-3

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 ConsumerElectronics Connectivity,Snapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon Industrial IOT,Snapdragon IoT, SnapdragonMobile, 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, SXR1130CVE 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1240

0-1

1-2

2-3

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SXR1130, SXR2130		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1241

0-1

1-2

2-3

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		
Improper Validation of Array Index	02-Nov-20	4.6	CVE ID : CVE-2020-11164 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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1242
			QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X,		

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

			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, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1243
Buffer Copy	02 Nov 20	10	u'Remote code execution can	https://w	H-QUA-MSM8-
without	02-Nov-20	10	happen by sending a	ww.qualco	181120/1244

731

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 Comsumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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/c ompany/p roduct- security/b ulletins/oc 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-MSM8- 181120/1245

0-1

1-2

2-3

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, 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	bulletin	
Improper Validation of Array Index	02-Nov-20	10	CVE ID : CVE-2020-3670 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1246

0-1

1-2

2-3

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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1247
			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	https://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-MSM8- 181120/1248

0-1

1-2

2-3

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1249

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1250

0-1

1-2

2-3

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 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 Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1252

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IDT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1253

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 Wearables, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1254
CVSS Scoring Scal	le 0-1	1-2	2-3 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-MSM8- 181120/1256

0-1

1-2

2-3

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 Wearables, 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, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-QCA6- 181120/1257

0-1

1-2

2-3

4-5

5-6

6-7

3-4

8-9

7-8

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, 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 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1258

0-1

1-2

2-3

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial 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, QCA6390, QCA6574AU, QCA6377, QCA9886, QCM6125, QCN7605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1259
CVSS Scoring Sca	le 0-1	1-2	2-3 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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-QCA6- 181120/1261

0-1

1-2

2-3

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 isaccessed from a tetheredclient through webserverdue to lack of array boundcheck.' in Snapdragon Auto,Snapdragon Compute,Snapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon Nobile,Snapdragon Wearables,Snapdragon Wearables,Snapdragon WiredInfrastructure andNetworking in APQ8009,APQ8017, APQ8053,APQ8096AU, APQ8098,IPQ4019, IPQ6018, IPQ8064,IPQ8074, MDM9150,MDM9206, MDM9207C,MDM9650, MSM8905,MSM8996AU, QCA6574AU,QCS405, QCS610, QRB5165,SC8180X, SDA660, SDA845,SDM429, SDM429W,SDM630, SDM632, SDM636,SDM660, SDM845, SDX20,SDX24, SDX55, SM8250 CVE ID : CVE-2020-3657	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
qcs405				L	
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-QCS4- 181120/1262

0-1

1-2

2-3

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, 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 Overfow 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1263

0-1

1-2

2-3

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, 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1264

0-1

1-2

2-3

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, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SXR1130, 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1265

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8905, 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 Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1266

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1267

0-1

1-2

2-3

<mark>3-4</mark> 750 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	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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1268
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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-QCS4- 181120/1269
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Nobile, 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, MSM8906AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1270

0-1

1-2

2-3

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 Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM898, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA45, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130		
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1271

0-1

1-2

2-3

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1273

0-1

1-2

2-3

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		
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 Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1274
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	CVE ID : CVE-2020-3690 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1276

0-1

1-2

2-3

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1277

0-1

1-2

2-3

<mark>3-4</mark> 757 4-5

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1278

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1279

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSS	Description & CVE ID SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125 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 Consumer IOT, Snapdragon Industrial IOT,	Patch	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-QCS6- 181120/1281

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	ompany/p roduct- security/b 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1282

0-1

1-2

2-3

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, SDM429W, SDM439,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1283

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8907, MSM8909W, MSM8917, 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, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDA6- 181120/1284

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-SDA6- 181120/1286
			validation' in Snapdragon Auto, Snapdragon Compute,	ulletins/oc tober-	

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDA6- 181120/1287

0-1

1-2

2-3

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		
Improper Validation of Array Index	02-Nov-20	4.6	CVE ID : CVE-2020-11164 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDA6- 181120/1288

0-1

1-2

2-3

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-SDA6- 181120/1290

0-1

1-2

2-3

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1291

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1292

0-1

1-2

2-3

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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Conpute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM89037, MSM8940,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1293

0-1

1-2

2-3

<mark>3-4</mark> 770 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 Wearables, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1294
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Industrial IOT, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SDM4- 181120/1296

0-1

1-2

2-3

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	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1297

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1298

0-1

1-2

2-3

<mark>3-4</mark> 774 4-5

5-6

6-7

7-8

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, 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, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1299
N/A	02-Nov-20	4.6	u'QSEE reads the access	https://w	H-QUA-SDM6-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			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 Nobile, 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/1300						
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 Overfow issue	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SDM6- 181120/1301						
		1.2									
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 776	CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10							

776

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 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, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, 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 Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SDM6- 181120/1302
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
CARR PLOT PLOT PLOT		1-2	2-3 3-4 4-5 5-6 777		0-9 9-10

777

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	bulletin	
			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 Mobile, Snapdragon Mobile, 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, MSM8906AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1303

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1304

0-1

1-2

2-3

4-5

5-6

6-7

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-SDM6- 181120/1306

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1307

0-1

1-2

2-3

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, 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1308

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1309

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1310

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 Wearables, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1311
CVSS Scoring Sca	le 0-1	1-2	2-3 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SDM6- 181120/1313

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1314

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM670,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1315

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8906AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 ww.qualco	H-QUA-SDX2-
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness bounds Read	Publish Date	CVSS	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, MDM9205, MDM9206, MDM9640, MDM9645, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	Patch mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	NCIIPC ID 181120/1317
			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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-SDX2- 181120/1318
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

790

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 Vired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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, SDM630, 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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX2- 181120/1319

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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 Noice & Music, Snapdragon Wiered 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Overfow issue (CVE-2019-16336,CVE-	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SDX2- 181120/1321

0-1

1-2

2-3

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, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, 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(C VE-2019-19193) mentioned	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SDX2- 181120/1322

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, Sicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, Sicobar, QCA6174A, Sicobar, QCA6174A, Sicobar, QCA6174A, Sicobar, QCA6174A, Sicobar, QCA6174A, Sicobar, QCA6174A, Sicobar, QCA6174A, Sicobar, QCA6574AU, Sicobar, QCA6174A, Sicobar, QCA6174A, Sicobar, QCA6174A, Sicobar, Sicoba Sicobar, Sicoba Sicobar, Sicoba Sicobar, Sicobar, Sicoba Sicobar, Sicobar, Sicoba Sicobar, Sicobar, S	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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SDX2- 181120/1323

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX2- 181120/1324

0-1

1-2

2-3

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, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250		
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, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1325

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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, 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1326

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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		
Out-of- bounds Write	02-Nov-20	4.6	CVE ID : CVE-2020-3684 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1327

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9650, MSM8905, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 ww.qualco	H-QUA-MDM9-
CVSS Scoring Sca	ale 0-1	1-2	2-3 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	mm.com/c	181120/1329
			message due to improper	ompany/p	
			length check of Information	roduct-	
			Element(IEI) NAS message	security/b	
			container' in Snapdragon	ulletins/oc	
			Auto, Snapdragon Compute,	tober-	
			Snapdragon Consumer IOT,	2020-	
			Snapdragon Industrial IOT,	bulletin	
			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		
			u'While processing invalid	https://w	
			connection request PDU	ww.qualco	
Improper			which is nonstandard	mm.com/c	H-QUA-MDM9-
Input	02-Nov-20	7.8	(interval or timeout is 0)	ompany/p	181120/1330
Validation			from central device may lead	roduct-	,
			peripheral system enter into	security/b	
			dead lock state.(This CVE is	ulletins/oc	
		1.2	2-3 3-4 4-5 5-6	6-7 7-8	80 040
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	0-7 /-8	8-9 9-10

800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, 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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-MDM9- 181120/1331

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1332

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Buffer Copy without (Classic Buffer Overflow')02-Nov-2010MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA4155P, Sapan, SC8180X, SDA660, SDA645, SDM429, SDM429W, SDM630, SDM630, SDM632, SDM636, SDM640, SDM630, SDM632, SDM636, SDM648, SDM20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130https://w wthe Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Wearables, Snapdragon Weirables, Snapdragon Weirables, Metworking in APQ8009, APQ807, APQ807, MDM9607, MDM9604, IPQ8074, MDM9510, MDM9607, MDM9640, MDM9606, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8906W, MSM8	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Image: construct of the security of the securi				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,		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')02-Nov-2010happen 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 Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8096AU, APQ8096A, IPQ4019, IPQ4019, IPQ4040, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8906AU, QCA6574AU, QCS405, QCS610, QRB5165,https://w 				CVE ID : CVE-2020-11174		
	without Checking Size of Input ('Classic Buffer	02-Nov-20	10	 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 Industrial IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8906AU, QCA6574AU, QCS405, QCS610, QRB5165, 	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

803

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 Wietal 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1334

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 Industrial IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Wired Snapdragon Wired Infrastructure and	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1336

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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, 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 Comsumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1337

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1338

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-3670 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 Nobile, 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, SDM630, SDM20, SM7150, SM8150, SM8250, SXR1130,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1339

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial 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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1340

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX2- 181120/1341

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Mobile, 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, MSM8906AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SDX2- 181120/1343
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 811	6-7 7-8	8-9 9-10

811

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, 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX2- 181120/1344

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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		
N/A	02-Nov-20	7.2	CVE ID : CVE-2020-3684 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 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX2- 181120/1345

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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX2- 181120/1346
			CVE ID : CVE-2020-3692		
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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX2- 181120/1347

0-1

1-2

2-3

4-5

5-6

6-7

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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Conpute, Snapdragon Congute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS404, QCS405, Rennell,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX2- 181120/1348
CVSS Scoring Scal	e 0-1	1-2	2-3 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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, 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, QCS404, QCS405, Rennell,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX2- 181120/1349
CVSS Scoring Scal	e 0-1	1-2	2-3 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	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 Woice Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM896AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-IPQ4- 181120/1351
CVSS Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

817

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 Woice & 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/b 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-IPQ4- 181120/1352

0-1

1-2

2-3

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, SM6150, SM7150, SM8150, SM8250, SXR2130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-IPQ4- 181120/1354

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ4- 181120/1355

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ4- 181120/1356

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-IPQ8- 181120/1358

822

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 Woice & 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/b 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-IPQ8- 181120/1359

0-1

1-2

2-3

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	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-IPQ8- 181120/1361

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ8- 181120/1362

0-1

1-2

2-3

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 u'Remote code execution can		
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 Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ8- 181120/1363

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-IPQ8- 181120/1365

827

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 Woice & 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/b 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-IPQ8- 181120/1366

0-1

1-2

2-3

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, SM6150, SM7150, SM8150, SM8250, SXR2130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-IPQ8- 181120/1368

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ8- 181120/1369

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 u'Remote code execution can		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	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 Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909W, MSM8953,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ8- 181120/1370

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial 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, QCA6174A, QCA9377,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1371

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Improper Input Validation02-Nov-207.87.87.87.87.8 CAS30, APA29, SDM420, SDM439, SDM439, SDM430, SDM4300, SDM430, SDM4300, SDM4300, SDM4300, SDM4300, SDM4300, SDM4300, SDM44	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation02-Nov-207.8Improper A Reserved Name Participation Page 2014 Page 2014 Page 2014 Page 2014 Page 2014 Page 2014 Page 2014u'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 Compute, Snapdragon Consumer Page 2014 Snapdragon Consumer Snapdragon Consumer 100T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, APQ8009, APQ8017, APQ8009, APQ8017, <b< td=""><td></td><td></td><td></td><td>QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130</td><td></td><td></td></b<>				QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130		
	Input	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 Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	

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 Industrial IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1373
qca9377				I	l
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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-QCA9- 181120/1374
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSS	Description & CVE ID from central device(This CVE is equivalent to Link Layer Length Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	Patch security/b ulletins/oc tober- 2020- bulletin	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	https://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-QCA9- 181120/1375

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SOM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704	ulletins/oc tober- 2020- bulletin	
qca9379					
Out-of-			u'Out of hourd more and	https://	
bounds Write	02-Nov-20	10	u'Out of bound memory access while processing GATT data received due to	https://w ww.qualco mm.com/c	H-QUA-QCA9- 181120/1376
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

836

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	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
			CVE ID : CVE-2020-11153		
sdm429w	Γ			Γ	
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, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1377

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1378

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1380

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1381
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Woice & 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, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-SDM4- 181120/1383

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1384

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1385

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-SDM4- 181120/1387

0-1

1-2

2-3

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 Woice & 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, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC71- 181120/1388

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

8-9

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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8907, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8953, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC71- 181120/1389

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-SC71- 181120/1391

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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	roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC71- 181120/1392
Improper Input	02-Nov-20	7.8	u'While processing invalid connection request PDU	https://w ww.qualco	H-QUA-SC71- 181120/1393

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			which is nonstandard	mm.com/c	
			(interval or timeout is 0)	ompany/p	
			from central device may lead	roduct-	
			peripheral system enter into	security/b	
			dead lock state.(This CVE is	ulletins/oc	
			equivalent to	tober-	
			InvalidConnectionRequest(C	2020-	
			VE-2019-19193) mentioned	bulletin	
			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		

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcm6125					
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, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM6- 181120/1394
Buffer Copy without Checking	02-Nov-20	10	u'Possible buffer overflow while updating output buffer for IMEI and Gateway	https://w ww.qualco mm.com/c	H-QUA-QCM6- 181120/1395

0-1

2-3

1-2

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	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
Out-of- bounds Read	02-Nov-20	7.5	CVE ID : CVE-2020-3692 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM6- 181120/1396

0-1

1-2

2-3

4-5

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8917, MSM8937, MSM8940, 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM6- 181120/1397

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1398

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1399
			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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1400

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 u'While processing invalid		
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 Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1401

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1402

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1403
			CVE ID : CVE-2020-11141 u'Buffer overflow while	https://w	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-APQ8- 181120/1404

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-APQ8- 181120/1406

0-1

1-2

2-3

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 Woice & Music, 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, SM6150, SM7150, SM8150, SM8250, SXR2130 	roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1407

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 Nobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1408
CVSS Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

860

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 Wietal Snapdragon Wieed Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-APQ8- 181120/1410
CVSS Scoring Scal	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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, MDM9645, MDM9645, MDM9645, MDM9650, MDM9645, MDM9653, MSM8909W, MSM8917, MSM8996AU, MSM8998, Nicobar, OWSM8998, Nicobar,ompany/p roduct- roduct- security/b ulletins/oc tober- 2020- bulletin	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				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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	roduct- security/b ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index02-Nov-2010u'Buffer overflow can happen as part of SIPhttps://w ww.qualco message packet processing while storing values in array due to lack of check tomm.com/c 181120/1411Validate the index length' in Snapdragon Auto,security/bH-QUA-APQ8- 181120/1411	Validation of	02-Nov-20	10	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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	• •
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CVSS Scoring Sca	le <u>0-1</u>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

862

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, 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1412

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1413
Use After Free	02-Nov-20	4.6	CVE ID : CVE-2020-3693 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-APQ8- 181120/1414

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1415

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1416
Improper	02-Nov-20	10	u'Buffer overflow occurs	https://w	H-QUA-APQ8-
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>

866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			while processing SIPmessage packet due to lackof check of index validationbefore copying into it' inSnapdragon Auto,Snapdragon Compute,Snapdragon Connectivity,Snapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon Wearables inAgatti, APQ8053,APQ8096AU, APQ8098,Bitra, Kamorta, MSM8905,MSM8909W, MSM8917,MSM8909W, MSM8917,MSM8940, MSM8953,MSM8996AU, MSM8998,Nicobar, QCA6390,QCA6574AU, QCM2150,QCS605, QM215, Rennell,SA6155P, SA8155P, Saipan,SDM429W, SDM439,SDM450, SDM630, SDM632,SDM450, SDM630, SDM632,SDM450, SDM630, SDM632,SDM710, SDM845, SM6150,SM7150, SM8150, SM8250,SXR1130, SXR2130 CVE ID : CVE-2020-3654	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/1417
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1418

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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			u'Detential out of hounds		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1419

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1420

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Out-of- bounds Read 02-Nov-20 7.5 SDM 429W, SDM439, SDM430, SDM630, SDM632, SDM450, SDM60, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 VE ID : CVE-2020-3673 Out-of- bounds Read 02-Nov-20 7.5 Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industria	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read02-Nov-207.57.5Substrate Bluetont peripheral firmware due to lack of check for invalid opcode and length of opcode received (CVE is equivalent to Link Layer Length Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overfow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in sweyntooth paper)' in smapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Source IDT, Snapdragon Industrial IOT, Source IDT, Snapdragon IDT, Snapdragon SOURCE, APQ8076, AR9344, Bitra, MSM8953, MSM8917, MSM8953, MSM8917, MSM8953, MSM8917, MSM8953, MSM8917, MSM8953, MSM8917, MSM8953, MSM8940, MSM8953, MSM8940,				SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
	bounds Read			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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/1421

870

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM950, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1422

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 Industrial IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Wearables, Snapdragon Wired	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1424

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1425

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM632, SDM636, SDM660, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1426

0-1

1-2

2-3

4-5

5-6

6-7 7-8

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-MSM8- 181120/1428

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1429

0-1

1-2

2-3

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, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1430

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1431

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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	ſ			ſ	
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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-NICO- 181120/1432

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-NICO- 181120/1434

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	tober- 2020- bulletin	
Use After Free	02-Nov-20	4.4	CVE ID : CVE-2020-11164 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-NICO- 181120/1435

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-NICO- 181120/1437

0-1

1-2

2-3

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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, 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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM350, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-NICO- 181120/1438

0-1

1-2

2-3

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, 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-NICO- 181120/1439

0-1

1-2

2-3

4-5

5-6

6-7

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-NICO- 181120/1441

0-1

1-2

2-3

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	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Nov-20	4.6	CVE ID : CVE-2020-3692 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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-NICO- 181120/1442
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-3693 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-NICO- 181120/1443

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130	ulletins/oc tober- 2020- bulletin	
			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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Consumer ICT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-NICO- 181120/1444
CVSS Scoring Sca	le 0-1	1-2	2-3 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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial 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, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-NICO- 181120/1445
CVSS Scoring Sca	le 0-1	1-2	2-3 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			CVE ID : CVE-2020-3704		
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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1447

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1449

0-1

1-2

2-3

4-5

5-6

6-7

3-4

8-9

7-8

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-APQ8- 181120/1451

0-1

1-2

2-3

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	ulletins/oc tober- 2020- bulletin	
			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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1452

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Improper Validation of Array Index02-Nov-2010<	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Indexu'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Ocnomute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Occe & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, MPQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ5018, IPQ6018, IPQ8064, UPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, SA8155P, Satan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM630, SDM632, SDM630, SDM630, SDM632, SDM630, SDM632, SDM630, SDM610, SDM10, SDM845, SDM22, SDM22, SDM210, SDM845, SDM20, SDM10, SDM845, SDM20, SDM20, SD						
Improper Validation of Array Index02-Nov-204.6issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Wearables, Snapdragon Wearables, Source, APQ8009, APQ8096AU, QCA9051, IPQ6018, IPQ8064, VEASI, VAC605, QCS605, SA4155N, SA6155P, Snapan, SC8180X, SDA660, SDM640, SDM640, SDM642, SDM640, SDM640, SDM642, SDM640, SDM640, SDM642, SDM640, SDM640, SDM642, SDM640, SDM640, SDM640, SDM640, SDM640, SDM640, SDM640, SDM640, SDM6				CVE ID : CVE-2020-11173		
Improper 02-Nov-20 10 u'Buffer overflow occurs https://w H-OUA-APO8-	Validation of	02-Nov-20	4.6	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 Nobile, Snapdragon Wieda 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	• •
	Improper	02-Nov-20	10	u'Buffer overflow occurs	https://w	H-QUA-APQ8-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			while processing SIPmessage packet due to lackof check of index validationbefore copying into it' inSnapdragon Auto,Snapdragon Compute,Snapdragon Connectivity,Snapdragon Industrial IOT,Snapdragon Mobile,Snapdragon Wearables inAgatti, APQ8053,APQ8096AU, APQ8098,Bitra, Kamorta, MSM8905,MSM8909W, MSM8917,MSM8940, MSM8917,MSM8940, MSM8953,MSM8996AU, MSM8998,Nicobar, QCA6390,QCA6574AU, QCM2150,QCS605, QM215, Rennell,SA6155P, SA8155P, Saipan,SDA660, SDM429,SDM450, SDM630, SDM632,SDM450, SDM630, SDM632,SDM450, SM8150, SM8250,SM7150, SM8150, SM8250,SXR1130, SXR2130 CVE ID : CVE-2020-3654	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/1454
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1455

0-1

1-2

2-3

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, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1456

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1457

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1458
			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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1459

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1460

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1461

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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 Woile, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-MDM9- 181120/1463
CVSS Scoring Scal	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

900

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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Conpute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM35, SNE(50, SM7150, SDM50, SXR1130	ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-MDM9- 181120/1464
CVSS Scoring Sca	le 0-1	1-2	2-3 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')			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 Woice & Music, 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	roduct- security/b ulletins/oc tober- 2020- bulletin	
msm8905					
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1465

0-1

1-2

2-3

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, 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		
Improper Validation of Array Index	02-Nov-20	10	CVE ID : CVE-2020-3670 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1466

0-1

1-2

2-3

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		
			u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents		
N/A	02-Nov-20	4.6	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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1467

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 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-MSM8- 181120/1469

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE is equivalent to Link Layer Length Overfow 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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, 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	ulletins/oc 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-MSM8- 181120/1470

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, 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, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1471

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Improper Validation of Array Index02-Nov-204.6Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSSM8937, MSM8940, MSM8933, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632https://w www.qualco mmroor of virar undex in Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, MEWORM, APQ8009, APQ8017, APQ809, APQ8017, APQ809, APQ8017, INFOS18, IPQ6018, IPQ8014, APQ8096, APQ8017, INDM9607, MDM9640, MDM9607, MDM9640, MDM9607, MDM9640, MDM9607, MDM9640, MDM9607, MDM9640, MDM9607, MDM9640, MDM9607, MDM9640, MDM9607, MDM9640, MDM9650, SNA89953, MSM8996AU, QCA6330, QCA9531, QCM2150, QCA9531, Q	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index02-Nov-204.6issue 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 Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9650, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X,Https://w ww.qualco mm.com/c orduct- security/b ulletins/cc tober- 2020- bulletinH-QUA-MSM8- 181120/1472				Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632		
	Validation of	02-Nov-20	4.6	 issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, 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, 	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-MSM8- 181120/1474

0-1

1-2

2-3

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 Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8906AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
qcn7605					
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-QCN7- 181120/1475

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, 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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SOM6125, 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	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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-QCN7- 181120/1476
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 911	6-7 7-8	8-9 9-10

911

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-QCN7- 181120/1478

0-1

1-2

2-3

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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-QCN7- 181120/1480

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	security/b ulletins/oc tober- 2020- bulletin	
			u'Buffer over-read while		
Integer Overflow or Wraparound	02-Nov-20	6.4	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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-SDM8- 181120/1482
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

					NCIIPC ID
			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, MDM9206, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index)2-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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-SDM8- 181120/1485

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

			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 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, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SXR1130, SXR2130 CVE ID : CVE-2020-3684	roduct- security/b ulletins/oc tober- 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM8- 181120/1486
	L L L L L L L L L L L L L L L L L L L				

917

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8940,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM8- 181120/1487

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM8- 181120/1488

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Out-of- bounds02-Nov-204.6u'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 Consumer 107, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Mobile, MILI20/1489H-QUA-SDM8- 181120/1489Ut-of- bounds02-Nov-204.6Ketworking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6330, QCA9331, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QR85155, Rennell, SA415M, SA515M, SA6155P, SA8155P, Sajpan,H-QUA-SDM8- ISI 120/1489	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Nov-204.6Anapen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto,https://w Napdragon Compute, Snapdragon Consumer I0T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Napdragon Voice & Music, Napdragon Wired Infrastructure and Networking in Agatti, HPQ8079, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA63390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M,H-QUA-SDM8- H-QUA-SDM8- IB				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		
	bounds	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 Wearables, 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, Rennell, SA415M, SA515M,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-

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		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	CVE ID : CVE-2020-11125 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 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, SM6150, SM7150, SM8150, SM8250, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM8- 181120/1490
			CVE ID : CVE-2020-11162		

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM8- 181120/1491
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	https://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-SDM8- 181120/1492

922

	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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	security/b ulletins/oc tober- 2020- bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	CVE ID : CVE-2020-3654 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 Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Snapdragon Wired Infrastructure and	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM8- 181120/1493

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, 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1494

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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 Industrial IOT, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1495

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ5- 181120/1496

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
Out-of- bounds Write	02-Nov-20	4.6	SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3704 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, 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, QCM215, QRB5165, Rennell, SA415M, SA515M,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ5- 181120/1497
			Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	5165, 515M, aipan, 0M660, 0M845, 150,	

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-IPQ5- 181120/1499

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ5- 181120/1500

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 ipcrtr as old one is deleted	https://w ww.qualco mm.com/c	H-QUA-APQ8- 181120/1502

930

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 Woice & 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, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24 CVE ID : CVE-2020-3696	ompany/p roduct- security/b ulletins/oc tober- 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 VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1503

0-1

1-2

2-3

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6125, QCN7605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1504

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, MSM8909W, MSM8953, QCA9531, 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 Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1505

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1506

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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		
			u'Buffer overflow can happen as part of SIP		
Improper Validation of Array Index	02-Nov-20	10	nappen 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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1507
Use After	02-Nov-20	4.6	u'Use after free while installing new security rule	https://w ww.qualco	H-QUA-APQ8- 181120/1508

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Woice & 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, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24	mm.com/c ompany/p roduct- security/b ulletins/oc 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, QCS605, Rennell, SA6155P,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1509

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1510

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-APQ8- 181120/1511
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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-APQ8- 181120/1512
Overflow')			due to lack of array bound check.' in Snapdragon Auto,	ulletins/oc tober-	

0-1

1-2

2-3

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, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDA8- 181120/1513

0-1

1-2

2-3

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, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-SDA8- 181120/1515

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SXR1130, SXR2130	roduct- security/b ulletins/oc tober- 2020- bulletin	
			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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDA8- 181120/1516

0-1

1-2

2-3

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDA8- 181120/1517

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Mobile, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDA8- 181120/1518

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDA8- 181120/1519
Buffer Copy	02-Nov-20	10	u'Remote code execution can	https://w	H-QUA-SDA8- 181120/1520

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 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, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
			CVE ID : CVE-2020-3657		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SDM6- 181120/1521

0-1

1-2

2-3

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, MSM898, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA45, SDM429, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1522

0-1

1-2

2-3

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		
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-3673 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1523

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1524

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-SDM6- 181120/1526

0-1

1-2

2-3

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, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, SA415M, SA515M, SA6155P, SA415M, SA515M, SA6155P, SA415M, SA515M, SA6155P, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM845, SDM632, SDM630, SDM845, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1527

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, 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 Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9206, MDM9207C, MDM9607, MDM9640,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1528

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1529

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 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, SDM450, SDM630, SDM632, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-SDM6- 181120/1531

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Size of Input ('Classic Buffor Overflow') init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Undustrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM670, SDM710, SDM845, SSR1130 outper- 2020- bulletin V 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 Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Industrial IOT, Snapdragon Otice & Music, Snapdragon Industrial IOT, Snapdragon Vired https://w ww.qualco mm.com/c ompany/p N/A 02-Nov-20 4.6 Affection (PG6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9450, SDM845, SDM630, SDM630, SDM660, SDM670, SDM710, SDM845, SDM630, SDM630, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, H-QUA-SDM6- 18120/1532	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
 N/A 02-Nov-20 4.6 MEM 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 Mobile, Napdragon Onsumer IOT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wired Snapdragon Wired Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, IPQ6018, Kamorta, IPG6018, Kamorta, 	('Classic 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	roduct- security/b ulletins/oc tober- 2020-	
	N/A	02-Nov-20	4.6	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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9205, MDM9650, MSM8905, SM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

954

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1534

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, 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		
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1535

0-1

1-2

2-3

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, 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		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1536

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1537

0-1

1-2

2-3

4-5

5-6

7-8

Improper Validation of Array Index02-Nov-204.6 A Array Index4.6 Array Index102-Nov-20 Array Index102-Nov-20 A	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Indexu'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Oconectivity, Snapdragon Notice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM89905, MSM89904, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS405, QCS405, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM632, SDM636, SDM646, SDM670, SDM70, SDM845, SDX20, SDX24, SDX55,Https://w wurduation H-QUA-SDM6- infrastructure and mr.com/c mm.com/c infrastructure and mm.com/c infrastructure and mm.com/c infrastructure and infrastructure a				SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55,	Validation of	02-Nov-20	4.6	SXR1130, SXR2130 CVE ID : CVE-2020-11164 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Wierd 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•
				SDM670, SDM710, SDM845, SDX20, SDX24, SDX55,		

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Improper Validation of Array Index02-Nov-2010SXR1130, SXR2130 CVE ID : CVE-2020-11174002-Nov-2010u'Buffer overflow occurs while processing SIP message packed due to lack of check of index validation before copying into it 'in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mubile, Snapdragon Mearables in Agatti, APQ8053, Bitra, Kamorta, MSM8905, MSM8990W, MSM8917, MSM8990W, MSM8917, MSM890W, MSM8917, MSM8990W, MSM8917, MSM890W, MSM8917, MSM8040, MSM8917, <br< th=""><th>Weakness</th><th>Publish Date</th><th>CVSS</th><th>Description & CVE ID</th><th>Patch</th><th>NCIIPC ID</th></br<>	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
Improper Validation of Array Index02-Nov-2010u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it 'in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, MSM8900 Kostnaptragon Consumer IOT, Snapdragon Mobile, www.qualco dgatti, APQ8053, MSM8996AU, APQ8098, mm.com/c orduct- security/b Ulletins/oc tober- 2020- UL-of- bounds ReadHttps://w ww.qualco mm.com/c orduct- security/b SDM450, SDM4290, SDM450, SDM450, SDM450, SDM450, SDM450, SDM450, SDM450, SDM450, SDM450, SDM640, SDM450, SDM450, SDM630, SDM632, SDM450, SDM640, SDM450, SDM450, SDM450, SDM630, SDM632, SDM450, SDM450, SDM630, SDM632, SDM450, SDM640, SDM450, SDM450, SDM450, SDM630, SDM632, SDM450, SDM450, SDM450, SDM450, SDM450, SDM640, SDM640, SDM450, SDM450, SDM640, SDM640, SDM450, SDM450, SDM640, SDM640, SDM450, SDM640, SDM640, <b< td=""><td></td><td></td><td></td><td>SXR1130, SXR2130</td><td></td><td></td></b<>				SXR1130, SXR2130						
Improper Validation of Array Index02-Nov-20Improper Validation of Array IndexImproper Validation				CVE ID : CVE-2020-11174						
sdm710 Out-of- 02-Nov-20 6.4 u'Potential out of bounds https://w ww.qualco downlink NAS transport mm.com/c mm.com/c H-QUA-SDM7- length check of Information roduct- 181120/1540 Element(IEI) NAS message security/b ulletins/oc	Validation of	02-Nov-20	10	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, MSM8917, MSM8940, MSM8953, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM6450, SM6150, SM7150, SM8150, SM8250,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•				
Out-of- bounds Read02-Nov-206.4u'Potential out of bounds read while processing downlink NAS transporthttps://w ww.qualco downlowH-QUA-SDM7- 181120/1540Iength check of Information Element(IEI) NAS message container' in Snapdragonsecurity/bH-QUA-SDM7- 181120/1540				CVE ID : CVE-2020-3654						
Out-of- bounds Read02-Nov-206.4read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragonww.qualco mm.com/c ompany/p roduct- ulletins/ocH-QUA-SDM7- 181120/1540	sdm710	sdm710								
		02-Nov-20	6.4	read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message	ww.qualco mm.com/c ompany/p roduct- security/b	e e				
	CVSS Scoring Sca	le 0-1	1-2	2-3 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, MDM9205, MDM9206, MDM9640, MDM9635M, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM7- 181120/1541

0-1

1-2

2-3

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM7- 181120/1542
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SDM7- 181120/1543

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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 Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM7- 181120/1544
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM7- 181120/1545

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM7- 181120/1546
CVSS Scoring Sca	le 0-1	1-2	2-3 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		
Out-of- bounds Write	02-Nov-20	4.6	CVE ID : CVE-2020-3704 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 Consumer IOT, Snapdragon Mobile, Snapdragon Nobile, 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, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM7- 181120/1547
CVSS Scoring Sca	le 0-1	1-2	SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, 2-3 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 Wietal 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, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-SDM7- 181120/1549

0-1

1-2

967

2-3

4-5

5-6

6-7

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	roduct- security/b 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 Industrial IOT, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM7- 181120/1550

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM670,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM7- 181120/1551

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1553

0-1

1-2

2-3

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	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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1554
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-QCS4- 181120/1555
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 971	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	tober- 2020- bulletin	
Out-of- bounds Read	02-Nov-20	7.5	CVE ID : CVE-2020-3690 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1556

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1557

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 u'Out of bound access can		
Out-of- bounds Write	02-Nov-20	4.6	happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1558

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-QCS4- 181120/1560

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS4- 181120/1561

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Improper Validation of Array Index02-Nov-204.6IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515H, SA6155P, SA8155P, Saipan, SC8180X, SDM429W, SDM632, SDM429W, SDM632, SDM429W, SDM632, SDM429W, SDM632, SDM429W, SDM632, SCM429W, SDM630, SDX55, SM6150, SXR2130Improper VEID : CVE-2020-11173U'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Werables, Snapdragon Werables, Snapdragon Werables, Snapdragon Werd Infrastructure and PQ8009, APQ8017, APQ8093, APQ8017, APQ8093, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9607, MDM9640	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index02-Nov-204.6issue 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 Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9650, MSM89050, MDM9650, MSM89050, MSM8996AU, QCA531, QCM2150, QCS404, QCS405, QCS405, QCS405, SA8155P, Saipan, SC8180X,H-QUA-QCS4- 181120/1562				MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130		
	Validation of	02-Nov-20	4.6	 issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, 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, 	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	• •

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, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, 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, SDM450, SDM630, SDM632,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR1- 181120/1563

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-SXR1- 181120/1565

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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/oc 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8905, SSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SXR1130,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR1- 181120/1566

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Overfow issue (CVE-2019-16336,CVE-	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SXR1- 181120/1568
			2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto,	2020- bulletin	

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR1- 181120/1569

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA63977, 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 Wired	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR1- 181120/1570

0-1

1-2

2-3

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, 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, SA8155P, Saipan, SDA660, SDM429W, SDM450,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR1- 181120/1571

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 u'Array index underflow		
Improper Validation of Array Index	02-Nov-20	4.6	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 Woice & 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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR1- 181120/1572

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SM61- 181120/1574

0-1

1-2

2-3

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, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM61- 181120/1575
CVSS Scoring Scal	le 0-1	1-2	2-3 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, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-SM61- 181120/1577

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, SSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM650, SDX20, SXR1130, SXR2130 CVE ID : CVE-2020-3684	ompany/p roduct- security/b ulletins/oc tober- 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SM61- 181120/1578

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, SDM670, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SM61- 181120/1580

0-1

1-2

2-3

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Overfow 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 Consumer	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM61- 181120/1582

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM61- 181120/1583

0-1

1-2

2-3

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6125, QCN7605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, 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 Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM61- 181120/1584

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM61- 181120/1585

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-SM61- 181120/1587

0-1

1-2

2-3

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 Woice & 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 Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM61- 181120/1588

0-1

1-2

2-3

4-5

5-6

6-7

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM61- 181120/1589

0-1

1-2

2-3

4-5

5-6

6-7

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM81- 181120/1591

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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,MSM8917, MSM8940,MSM8953, MSM8996AU,MSM8953, MSM8996AU,MSM898, Nicobar,QCM2150, QCM6125,QCS605, QCS610, QM215,Rennell, SA415M, Saipan,SC7180, SC8180X, SDA660,SDA459, SDM429,SDM429W, SDM439,SDM450, SDM630, SDM632,SDM636, SDM660, SDM670,SDX20, SDX24, SDX55,SM6150, SM7150, SM8150,SXR1130CVE 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM81- 181120/1592

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

N/A02-Nov-204.6MSM899AU, MSM8953, MSM8996AU, Nicobar, QCA3930, QCA657AU, QCA657AU, QCA657AU, QCA657AU, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM630, SDM630, SDM632, SDM636, SDM660, SDM429, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130Https://w www.ualco mm.com/c ompany/p roduct- sapdragon Consumer 107, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9205, MDM9205, MDM9206, MDM9205, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9510, MDM9205, MSM8996, SSM8390, Scobar, QCA6390, QCS404, QCS405, QCA6390, QCS404, QCS405, QCA6390, QCS404, QCS405, SDM630, SDM630, SDM636, SDM660,H-QUA-SM81- H-QUA-SM81- 181120/1593	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A02-Nov-204.6u'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 Consumer IOT, Snapdragon Molie,https://w www.qualco mm.com/c ompany/p roduct- security/b 181120/1593N/A02-Nov-204.6Snapdragon Molie, Snapdragon Wired Infrastructure and Networking in Agatti, IPQ6018, Kamorta, IPQ6018, Kamorta, QCA6390, QCS404, QCS405, QCS605, QCS510, Rennell, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845,H-QUA-SM81- H-QUA-SM81- 181120/1593				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		
	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 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	e

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		
			u'Due to an incorrect SMMU		
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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM81- 181120/1594
				https://w	
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM81- 181120/1595

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM81- 181120/1597

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9 **9-1**0

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM81- 181120/1598

0-1

1-2

2-3

4-5

5-6

6-7

3-4

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM81- 181120/1599

0-1

1-2

2-3

4-5

6-7

5-6

8-9 9-10

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-SM81- 181120/1601

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	ompany/p roduct- security/b ulletins/oc 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM81- 181120/1602

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM81- 181120/1603

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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	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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM81- 181120/1604
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack	https://w ww.qualco mm.com/c	H-QUA-SM81- 181120/1605

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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	ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1606

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

8-9

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,MSM8917, MSM8940,MSM8953, MSM8996AU,MSM898, Nicobar,QCM2150, QCM6125,QCS605, QCS610, QM215,Rennell, SA415M, Saipan,SC7180, SC8180X, SDA660,SDA845, SDM429,SDM429W, SDM439,SDM450, SDM630, SDM632,SDM636, SDM660, SDM670,SDX20, SDX24, SDX55,SM6150, SM7150, SM8150,SXR1130CVE 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1607

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, 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, 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1608

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1609

0-1

1-2

2-3

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, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MDM9- 181120/1610

0-1

1-2

2-3

4-5

5-6

6-7

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		
qca9531			CVE ID : CVE-2020-3670		
			u'Use after free while installing new security rule in ipcrtr as old one is deleted and this rule could still be in		
Use After Free	02-Nov-20	4.6	use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-QCA9- 181120/1612
CVSS Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6 1014	6-7 7-8	8-9 9-10

1014

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 Woice & 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/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-QCA9- 181120/1613

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA9- 181120/1614
qca9886					
Improper Input	02-Nov-20	7.8	u'While processing invalid connection request PDU	https://w ww.qualco	H-QUA-QCA9- 181120/1615
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 1016	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			which is nonstandard	mm.com/c	
			(interval or timeout is 0)	ompany/p	
			from central device may lead	roduct-	
			peripheral system enter into	security/b	
			dead lock state.(This CVE is	ulletins/oc	
			equivalent to	tober-	
			InvalidConnectionRequest(C	2020-	
			VE-2019-19193) mentioned	bulletin	
			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		

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA9- 181120/1617
qm215			I		
Out-of- bounds Read	02-Nov-20	6.4	u'Potential out of bounds read while processing downlink NAS transport	https://w ww.qualco mm.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

Improper Validation of Array Index02-Nov-200102020203040405040504UXSS Scoring Scate02-Nov-2001122334455657788990	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index02-Nov-2010happen 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,mm.com/c ompany/p tober-H-QUA-QM21- 181120/16191010Snapdragon Auto, Snapdragon Compute,ulletins/oc				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, MDM9205, MDM9206, MDM9640, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	roduct- security/b ulletins/oc tober- 2020-	
	Validation of	02-Nov-20	10	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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	• •
	CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1019

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, 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QM21- 181120/1620

0-1

1-2

2-3

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, 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 Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QM21- 181120/1621

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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		
Improper Input Validation	02-Nov-20	5	CVE ID : CVE-2020-11125 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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QM21- 181120/1622

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Mobile, Snapdragon Nobile, 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, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID: CVE-2020-11162 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-QM21- 181120/1624

0-1

1-2

2-3

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM71- 181120/1625

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM71- 181120/1626
Improper	02-Nov-20	10	u'Buffer overflow can	https://w	H-QUA-SM71-
Validation of			happen as part of SIP	ww.qualco	181120/1627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			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, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	mm.com/c ompany/p roduct- security/b ulletins/oc 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM71- 181120/1628

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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		
N/A	02-Nov-20	7.2	CVE ID : CVE-2020-3684 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 Industrial IOT, Snapdragon Mobile, 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM71- 181120/1629

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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM71- 181120/1630
			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 Overfow 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 Consumer Electronics Connectivity,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM71- 181120/1631

0-1

1-2

2-3

4-5

5-6

6-7

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, 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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM71- 181120/1632

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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 Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM71- 181120/1633

0-1

1-2

2-3

4-5

5-6

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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM71- 181120/1634

0-1

1-2

2-3

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		
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-11162 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-SM71- 181120/1636

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM71- 181120/1637

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1638

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8940, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM896AU, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1639
Out-of-	02-Nov-20	7.5	u'Buffer over-read issue in	https://w	H-QUA-SDM4-
bounds Read	02-1107-20	7.5	Bluetooth peripheral	ww.qualco	181120/1640
CVSS Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Conpute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, 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	mm.com/c 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 process due to lack of check	https://w ww.qualco mm.com/c	H-QUA-SDM4- 181120/1641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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	ompany/p roduct- security/b ulletins/oc 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SDM4- 181120/1642

1037

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, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632	2020- bulletin	
			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 Industrial IOT, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1643

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	CVE ID : CVE-2020-11162u'Two threads runningsimultaneously from userspace can lead to racecondition in fastRPC driver'in Snapdragon Auto,Snapdragon Compute,Snapdragon Connectivity,Snapdragon Consumer IOT,Snapdragon Consumer IOT,Snapdragon Mobile,Snapdragon Mobile,Snapdragon Wearables,Snapdragon WiredInfrastructure andNetworking in Agatti,APQ8053, Bitra, IPQ4019,IPQ5018, IPQ6018, IPQ8064,IPQ8074, Kamorta,MDM9607, MSM8953,Nicobar, QCA6390, QCS404,QCS405, QCS610, Rennell,SA515M, SA6155P,SA8155P, Saipan, SC8180X,SDM429W, SDM632,SDM429W, SDM632,SDM660, SDX55, SM6150,SM7150, SM8150, SM8250,SXR2130CVE ID : CVE-2020-11173	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-SDM4- 181120/1645

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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, 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	roduct- security/b ulletins/oc tober- 2020- bulletin	
Improper Validation of Array Index	02-Nov-20	10	CVE ID : CVE-2020-11174 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SDM4- 181120/1646

0-1

1-2

2-3

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, 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 Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1647

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
sdm632			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, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1648

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 Consumer IOT, 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, SDM450, SDM630, SDM632, SDM450, SDM630, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3673	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1649

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8937, NSM8940, 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1650

0-1

1-2

2-3

4-5

5-6

6-7

3-4

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-SDM6- 181120/1652

1045

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 Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632	security/b ulletins/oc tober- 2020- bulletin	
			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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1653

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wieda 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1654
Improper	02-Nov-20	4.6	u'Array index underflow	https://w	H-QUA-SDM6-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			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 Nobile, Snapdragon Woice & 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/1655
			u'Buffer overflow occurs	https://w	
Improper Validation of Array Index	02-Nov-20	10	while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto,	ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-SDM6- 181120/1656
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, 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 Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM6- 181120/1657

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1658

0-1

1-2

2-3

4-5

5-6

7-8

6-7

9-10

Improper Validation of Array Index02-Nov-2010QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC1800, SDM630, SDM630, SDM429, SDM439, SDM429, SDM430, SDM630, SDM632, SDM430, SDM630, SDM630, SDM632, SDM430, SDM430, SDM630, SDM630, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130Https://w www.qualco mm.com/c ompany/pImproper Validation of Array Index02-Nov-2010UBUfer 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 Consumer 107, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Quota, PQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8904, NisM8917, MSM8904, NisM8917, MSM8904, NisM8917, MSM8904, NisM8917, MSM8904, NisM8917, MSM8904, NisM8917, MSM8904, NisM8917, SDM420, QCA6139, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM430, SDM630, SDM632, SDM430, SDM630, SDM630, SDM632, SDM430, SDM630, SDM632, SDM430, SDM630, SDM632,	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index02-Nov-2010u'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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Magett, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8906AU, Nicobar, QCA6390, QCA6577AU, QCA6390, QCA6575AU, QCA6155P, SAB155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM630, SDM450, SDM630, SDM				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		
	Validation of	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, 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Overfow 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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8953, Nicobar, QCA6174A, QCA9377, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1660

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

			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 Industrial IOT, Snapdragon Woice & Music, 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, SDM429W, SDM439, SDM450, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1661
Improper	02-Nov-20	5	u'Lack of handling	https://w	H-QUA-MSM8- 181120/1662
Input			unexpected control	ww.qualco	101120/1002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			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 Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8933, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632 CVE ID : CVE-2020-11157	mm.com/c ompany/p roduct- security/b 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 Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1663

0-1

1-2

2-3

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-MSM8- 181120/1665
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1055

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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	ompany/p roduct- security/b ulletins/oc tober- 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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1666

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1667
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1057

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-MSM8- 181120/1669						
CVSS Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8							

1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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, 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1670

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-MSM8- 181120/1671
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-MSM8- 181120/1673

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

CVE is equivalent to Linkulletins/ocLayer Length Overfow issuetober-(CVE-2019-16336,CVE-2020-2019-17519) and SilentbulletinLength Overflow issue(CVE-2019-17518) mentioned in	
(CVE-2019-16336,CVE- 2020- 2019-17519) and Silent bulletin Length Overflow issue(CVE- 2019-17518) mentioned in	
2019-17519) and Silent bulletin Length Overflow issue(CVE- 2019-17518) mentioned in	
Length Overflow issue(CVE- 2019-17518) mentioned in	
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	
sdm450	
u'Potential out of bounds https://w	
read while processing	SDM4
02-Nov-20 64 downlink NAS transport mm com/c	-SDM4-
message due to improper ompany/p	0/1674

0-1

1-2

2-3

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, MDM9205, MDM9206, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SDM4- 181120/1675

0-1

1-2

2-3

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1676

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1677

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

		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 Industrial IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 ww.qualco	H-QUA-SDM4- 181120/1679

0-1

1-2

2-3

4-5

5-6

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 Woice & 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/c ompany/p roduct- security/b ulletins/oc 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM4- 181120/1680		
CVSS Scoring Sca		1-2	7 -3 3-4 4-5 5-6	6-7 7.9	8-9 9-10		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 1067							

1067

Improper Validation of Array Index02-Nov-2010Agatti, APQ80996, Bitra, Kamorta, MSM89090, MSM8917, MSM8900, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Sa8155P, Sashan, SDM660, SDM429W, SDM450, SDM670, SDM710, SM6150, SM7150, SM8250, SXR1130, SXR2130Hereice CVE ID : CVE-2020-11164U'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer 107, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Mobile, MSM8906AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM89040, MSM8953, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM89040, MSM8953, MSM8909W, MSM8917, MSM89040, MSM8953, MSM89040, MSM8953, MSM89040, MSM8953, MSM89040, MSM8953, MSM89040, MSM8953, MSM89040, MSM8953, MSM89040, MSM8953, MSM89040, MSM8953, MSM8040, MSM8953, SDM420, SDM	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index02-Nov-2010Network with the processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Magatti, APQ8053, MSM8906AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8996AU, MSM8917, MILetins/oct MSM8996AU, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8953, MSM896AU, MSM898, SDA660, SDM4210, SDA660, SDM429, SDM450, SDM450, SDM450, SDM450, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150,H-QUA-SDM4- H-QUA-SDM4- 181120/1681 WW.QUAICO WW.QUAICO WW.QUAICO WW.QUAICO WW.QUAICO				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		
SM7150, SM8150, SM8250,	Validation of	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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM660, SDM670,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130		
			CVE ID : CVE-2020-3654		
sm8250	l				
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM82- 181120/1683

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

N/A02-Nov-204.6NSM8996AU, NSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM630, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130Https://w WW2020-3673VI 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Voice & Music, NP9009, APQ8098, Bitra, IPQ6018, Kamorta, IPQ6018, Kamorta, IPQ6018, Kamorta, IPQ6018, Kamorta, IPQ6018, Kamorta, IPQ6018, Kamorta, IPQ6018, Kamorta, IPQ6018, Kamorta, IPQ6019, APQ8098, Bitra, IPQ6018, Kamorta, IPQ6018, Kamorta, IPQ601	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A02-Nov-204.6u'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 Connectivity, Snapdragon Connectivity, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music, Ompany/p roduct- Infrastructure and NPM9150, MDM9205, MDM9150, MDM9205, MDM9500, MDM9205, MDM9206, MDM9205, MDM9206, MDM9205, MDM9206, MDM9205, MDM9206, MDM9205, MDM9206, MDM9205, MDM9500, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, SA8155P, SA8				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		
	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 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM82- 181120/1686

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM82- 181120/1688

0-1

1-2

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial 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, QCA6390, QCA6574AU, QCA6377, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM82- 181120/1689

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Wireid 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, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM82- 181120/1690
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	https://w ww.qualco mm.com/c	H-QUA-SM82- 181120/1691

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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 Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250	ompany/p roduct- security/b ulletins/oc 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 Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco	H-QUA-SM82- 181120/1693

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, 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, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2020-11162	mm.com/c ompany/p roduct- security/b ulletins/oc 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM82- 181120/1694	
CVSS Scoring Sca	le 0-1	1-2	7 -3 3-4 4-5 5-6	6-7 7.8	8-9 9-10	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 1076						

1076

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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM82- 181120/1695

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8909W, MSM8953, MSM8906AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM632, SDM636, SDM660, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM82- 181120/1696
Improper Validation of	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://w ww.qualco	H-QUA-SM82- 181120/1697
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	mm.com/c ompany/p roduct- security/b 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SM82- 181120/1698

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Woile, Snapdragon Woile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR2- 181120/1699

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR2- 181120/1700

0-1

1-2

2-3

4-5

5-6

6-7

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SXR2- 181120/1702

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR2- 181120/1703

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
Incorrect Default Permissions	02-Nov-20	4.6	CVE ID : CVE-2020-11174 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-SXR2- 181120/1705

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR2- 181120/1706

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

N/A02-Nov-204.6Bitra, Kamorta, MSM8905, MSM890W, MSM8917, MSM890W, MSM8917, MSM8990, QCA6574AU, QCA6390, QCA6574AU, QCM2150, QCS005, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM430, SDM630, SDM632, SDM630, SDM630, SDM632, SDM630, SDM630, SDM630, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR130Https://w www.ualca ompany/p roduct- scurity/ Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9206, MDM9607, MDM950, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Sajan, SC7180,H-QUA-SXR2- ISI20/1707	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A02-Nov-204.6u'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 Consumer 10T, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and ulletins/oct HPQ8009, APQ8098, Bitra, ID6018, Kamorta, MDM9150, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P,Image and applies and applies and applies and applies and applies and applies them without validation' in Snapdragon wetworking in Agatti, tober-https://wN/A02-Nov-204.6H-QUA-SXR2- Snapdragon Voice & Music, Snapdragon Wired Infrastructure and MDM9150, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MDM9205, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P,Image and applies and				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		
	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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

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 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, SDM670, SDM710, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR2- 181120/1708
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	CVE ID : CVE-2020-3690 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SXR2- 181120/1709

0-1

1-2

2-3

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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR2- 181120/1710
			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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR2- 181120/1711

0-1

1-2

2-3

4-5

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial 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, QCA6390, QCA6574AU, QCA6377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS404, QCS405, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SXR2- 181120/1712

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA61- 181120/1713

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA61- 181120/1715

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155 u'Possible buffer overflow in		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	u Possible buffer överflöw 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 Wietal 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-SA61- 181120/1717

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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/b ulletins/oc tober- 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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA61- 181120/1718

0-1

1-2

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	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 Wearables, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA61- 181120/1719
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA61- 181120/1720

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA61- 181120/1721

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, 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, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA61- 181120/1722

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Consumer IOT, Snapdragon Mobile, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM950, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-SA61- 181120/1724

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	roduct- security/b ulletins/oc tober- 2020- bulletin	
sc8180x					
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC81- 181120/1725

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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	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, MDM9205, MDM9206, MDM9640, MDM9645, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8953, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-SC81- 181120/1727

0-1

1-2

2-3

4-5

5-6

6-7

7-8

			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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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	ompany/p roduct- security/b ulletins/oc tober- 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SC81- 181120/1728
	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1100

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, SDM670, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Overfow issue	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SC81- 181120/1730

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

(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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM89037, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM430, SDM430, SDM450, SDM630, SDM632, SDM450, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM630, SDM632, SDM450, SDM630, SDM630, SDM630, SDM630, SDM450, SDM630	Weakness	Patch NCIIPC I	CVSS Description & CVE ID	NCIIPC ID
SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703		bulletin VE- l in y, , OT, OT, OT, OT, agon e & , , 5, l, 439, 532, 570, 0,), 3	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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, 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 Input02-Nov-207.8u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0)ww.qualco mm.com/c ompany/p roduct- 181120/173Validation02-Nov-207.8from central device may lead dead lock state.(This CVE is equivalent to InvalidConnectionRequest(Culletins/oc 2020-H-QUA-SC81- 181120/173	Input	ww.qualco mm.com/c ompany/p lead roduct- into security/b E is ulletins/oc tober-	 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 	•
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-	CVSS Scoring Sca	5-6 6-7 7-8 8-9	2 2-3 3-4 4-5 5-6	8-9 9-10

1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, 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	bulletin	
			cve ID : cve-2020-3704 u'Out of bound access can	https://w	
Out-of- bounds Write	02-Nov-20	4.6	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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SC81- 181120/1732
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC81- 181120/1733

0-1

1-2

2-3

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	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 Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55 CVE ID : CVE-2020-11153	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC81- 181120/1734
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC81- 181120/1735

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9 **9-1**0

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC81- 181120/1737

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wearables, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC81- 181120/1738

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC81- 181120/1740

0-1

1-2

2-3

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC81- 181120/1741
CVSS Scoring Scal	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1109

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 Nobile, Snapdragon Wieta Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SC81- 181120/1742

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdm850					
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, MDM9645, MDM9650, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM130 CVE ID : CVE-2020-3670	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM8- 181120/1743
N/A	02-Nov-20	4.6	u'QSEE reads the access permission policy for the SMEM TOC partition from	https://w ww.qualco mm.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
			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 Noice & 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, SDM710, SDM845, SDM630, SDM710, SDM845, SDM630, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	ompany/p roduct- security/b ulletins/oc tober- 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SDM8- 181120/1745
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
CARR PLANE SCA		1-2	2-3 3-4 4-5 5-6 1112	1-8	0-9 9-10

1112

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, SDM670, 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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDM8- 181120/1746

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9640, MDM9645, MDM9650, MDM9645, MDM9650, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM2- 181120/1747

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM2- 181120/1748

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM2- 181120/1750

0-1

1-2

2-3

4-5

5-6

6-7

7-8 8-9

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM2- 181120/1751
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM2- 181120/1752

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Industrial IOT, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Wearables, Snapdragon Wired	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM2- 181120/1754

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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		
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-11162 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM2- 181120/1755

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCM2- 181120/1756
Improper Validation of	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://w ww.qualco	H-QUA-QCM2- 181120/1757
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
sdx55					
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1758

0-1

1-2

2-3

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, MDM9645, MDM9650, MDM9645, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1759
CVSS Scoring Scal	e 0-1	1-2	2-3 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9607, MDM9206, MDM9607, MDM950, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM650, SM220, SXR1130, SXR2130 CVE ID : CVE-2020-3684	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1760
N/A	02-Nov-20	7.2	u'Due to an incorrect SMMU configuration, the modem	https://w ww.qualco	H-QUA-SDX5- 181120/1761

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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, SDM650, SM7150, SM8150, SM8250, SXR1130, SXR2130	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1762

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial 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, QCA6390, QCA6574AU, QCA6377, QCA9886, QCM6125, QCN7605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SXZ4, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1763

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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	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 Wiered 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, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11125	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1764
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	https://w ww.qualco mm.com/c	H-QUA-SDX5- 181120/1765

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Wirel Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-SDX5- 181120/1767

0-1

1-2

2-3

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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	roduct- security/b ulletins/oc tober- 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 Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11155	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1768

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1769
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 Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1770

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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		
Integer Overflow or Wraparound	02-Nov-20	6.4	CVE ID : CVE-2020-11162 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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SDX5- 181120/1772

0-1

1-2

2-3

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1773

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SDX5- 181120/1774

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-AR93- 181120/1775

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-AR93- 181120/1776
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1135

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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in AR9344	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-AGAT- 181120/1778
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1136

Buffer Copy without (Classic Buffer Copy without (Classic Buffer Copy without (Classic Buffer Copy without (Classic Buffer Overflow')Snapdragon Werables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6064, IPQ8074, Kamorta, MDM9550, MSM8905, MSM89150, MM89053, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS404, QS405, SDM429, SDM429, SDM429, SDM429, SDM450, SM620, SM710, SM8150, SM8150, SM8150, SM8150, SM8150, SM8250, SM8150, SM8250, SM8150, SM8250, SM8150, SM8250, SM8150, SM8250, SM8150, SM8250, SM2510, SM8150, SM8250, SM250, SM8150, SM8250, SM250, SM8150, SM8150, SM8250, SM250, SM8150, SM8250, SM250, SM8150, SM8250, SM250, SM8150, SM8250, SM250, SM250, SM250, SM8150, SM8250, SM250, SM8150, SM8250, SM250, SM8150, SM8250, SM250, SM8150, SM8250, SM250, SM250	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')02-Nov-204.6MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti,https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletinH-QUA-AGAT- 181120/1779				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		
AI (0000), DIU a, II (401),	without Checking Size of Input ('Classic Buffer	02-Nov-20	4.6	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 Wired Snapdragon Wired Infrastructure and	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	e

IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130CVE ID : CVE-2020-11162u'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,				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,		
u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto,Image: Control of the second secon				SM6150, SM7150, SM8150,		
call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto,						
N/A 02-Nov-20 4.6 Snapdragon Consumer IOT, https://w Snapdragon Industrial IOT, www.qualco Snapdragon Mobile, mm.com/c Snapdragon Wearables in ompany/p Agatti, APQ8096AU, roduct- H-QUA-AGA	N/A C	Ϋ́Α 02-Νο	v-20 4.6	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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-AGAT- 181120/1780
Use After 02-Nov-20 4.4 u'Two threads running https://w H-QUA-AGA	Use After 0	se After 02-No	v-20 4.4	u'Two threads running	https://w	H-QUA-AGAT-

0-1

1-2

2-3

3-4 1138 4-5

5-6

7-8

6-7

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 Woice & 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Wired	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-AGAT- 181120/1782

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-AGAT- 181120/1783

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-AGAT- 181120/1785

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-AGAT- 181120/1786
			onaparagon it carabico m		I

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-AGAT- 181120/1788

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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 Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-AGAT- 181120/1789
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1144

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-AGAT- 181120/1791

0-1

1-2

2-3

4-5

5-6

6-7

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6125, QCN7605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
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(C VE-2019-19193) mentioned in sweyntooth paper)' in	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QRB5- 181120/1792

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6125, QCN7605, QCS404, QCS405, QCS605, QCS404, QCS405, QCS605,<		
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-QRB5- 181120/1793

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	CVE ID : CVE-2020-11125 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QRB5- 181120/1794

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	CVE ID : CVE-2020-11162 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 Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QRB5- 181120/1795

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-QCN7- 181120/1797

1150

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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-RENN- 181120/1799
CVSS Scoring Scal	le 0-1	1-2	2-3 3-4 4-5 5-6 1151	6-7 7-8	8-9 9-10

	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	roduct- security/b ulletins/oc 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, MDM9206, MDM9640, MDM9645, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-RENN- 181120/1800

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-RENN- 181120/1801

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-RENN- 181120/1802
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,	https://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-RENN- 181120/1803

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c	H-QUA-RENN- 181120/1805

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8905, MSM8917, MSM8905, MSM8917, MSM8953, Nicobar, QCA6174A, QCA9377, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3703	ompany/p roduct- security/b ulletins/oc tober- 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)	https://w ww.qualco mm.com/c ompany/p	H-QUA-RENN- 181120/1806
CVSS Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1156

Out-of- bounds02-Nov-204.6diamon with the second seco	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Nov-204.6happen in MHI commandww.qualcoH-Q0A-RENN- 181120/1807				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 Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial 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, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS404, QCS405, QCS605, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM7150, SM8150, SM8250, SXR1130, SXR2130	security/b ulletins/oc tober- 2020-	
		02-Nov-20	4.6	happen in MHI command	ww.qualco	•

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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	ompany/p roduct- security/b 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-RENN- 181120/1808

1158

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-RENN- 181120/1809

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-RENN- 181120/1811

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA41- 181120/1812

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA41- 181120/1813

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA41- 181120/1814
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	CVE ID : CVE-2020-11154 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA41- 181120/1815

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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 Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA41- 181120/1817

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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		
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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11169	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA41- 181120/1818

0-1

1-2

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	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 Nobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA41- 181120/1819
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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-SA41- 181120/1820
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 1166	6-7 7-8	<u>8-9</u> 9-10

1166

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 CVE ID : CVE-2020-3670	security/b ulletins/oc 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SA41- 181120/1821
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1167

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 Industrial IOT, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA41- 181120/1822

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA41- 181120/1824

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCS404, QCS405, QCS605, 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		
saipan					
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SAIP- 181120/1825

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

8-9 9-10

Improper Validation of Array Index02-Nov-2010Agatti, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9655, MDM96353, MSM8905, MSM8909W, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8995, MSM8909W, MSM8995, MSM8909W, MSM8905, SDM509, QCS610, QM215, QCS605, QCS610, QM215, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SCB180X, SDA660, SDA429, SDM450, SDM430, SDM429, SDM439, SDM429, SDM430, SDM632, SDM430, SDM632, SDM630, SDM632, SDM430, SDM630, SDM632, SDM430, SDM630, SDM632, SDM450, SDM710, SDM845, SDM850, SXR1130https://w ww.qualco mm.com/c ompany/p roduct sapdragon Auto, Snapdragon Consumer 107, Snapdragon Industrial 107, Snapdragon Industrial 107, Snapdragon Industrial 107, Snapdragon Industrial 107, Snapdragon Industrial 107, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Meables in Agetti, APQ8053, APQ80540, APQ8098, Bitra, Kamorta, MSM8905, MEM0207, MCM0177, MCM017, MCM017,	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index02-Nov-2010happen 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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905,https://w ww.qualco mm.com/c ompany/p roduct- security/b 2020- bulletinH-QUA-SAIP- 181120/1826				APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, 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		
M5M8909W, M5M8917,	Validation of	02-Nov-20	10	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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

N/A02-Nov-204.6MSM89940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM600, SDM630, SDM630, SDM710, SDM8150, SM8250, SXR1130, SXR2130VVEVE ID : CVE-2020-3673u'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 Compute, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and NDM9150, MDM9205, MDM9206, MDM9205, MDM9150, MDM9205, MDM9206, MSM8905, MSM8990, QCS404, QCS405, QCS605, QCS605, QCS604, SDM630, S	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A02-Nov-204.6u'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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Molie,https://w www.qualco ommany/p roduct- 181120/1827N/A02-Nov-204.6Snapdragon Wired Infrastructure and NEWorking in Agatti, IPQ6018, Kamorta, IPQ6018, Kamorta, QCA6390, QCS404, QCS405, QCX6607, MDM9205, MDM9205, MDM9505, MSM89988, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS510, Rennell, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845,H-QUA-SAIP- H-QUA-SAIP- 181120/1827				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		
	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 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-

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 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SAIP- 181120/1829

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SAIP- 181120/1831

0-1

1-2

2-3

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, 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, QCA6390, QCA6574AU, QCA6377, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SAIP- 181120/1832

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Wiered 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, QCS404, QCS405, QCS605, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SAIP- 181120/1833
Buffer Copy without	02-Nov-20	4.6	u'Possible buffer overflow in MHI driver due to lack of	https://w ww.qualco	H-QUA-SAIP- 181120/1834

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Size of Input ('Classic Buffer			of EOT events received from		1
Overflow')			MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
N/A 0	92-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SAIP- 181120/1835
· I	_				

1177

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SAIP- 181120/1836

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SAIP- 181120/1837
Improper Validation of Array Index	02-Nov-20	10	u'Buffer overflow occurs while processing SIP message packet due to lack	https://w ww.qualco mm.com/c	H-QUA-SAIP- 181120/1838

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	ompany/p roduct- security/b ulletins/oc tober- 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 Industrial IOT, Snapdragon Mobile,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ6- 181120/1839

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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 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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ6- 181120/1840

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ6- 181120/1841
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Nobile, Snapdragon Nobile, Snapdragon Wierdal IOT, 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, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID: CVE-2020-11162 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b	H-QUA-IPQ6- 181120/1843

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-IPQ6- 181120/1845

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8906AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-IPQ6- 181120/1846

0-1

1-2

2-3

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, 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 Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-KAMO- 181120/1847

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-KAMO- 181120/1848

0-1

1-2

2-3

4-5

5-6

6-7

7-8

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-KAMO- 181120/1850

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-KAMO- 181120/1851

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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		
Incorrect Default Permissions	02-Nov-20	4.6	CVE ID : CVE-2020-11174 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-KAMO- 181120/1852
Improper			u'Buffer overflow occurs	https://w	
Validation of Array Index	02-Nov-20	10	while processing SIP message packet due to lack	ww.qualco mm.com/c	H-QUA-KAMO- 181120/1853

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	ompany/p roduct- security/b ulletins/oc 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-KAMO- 181120/1854

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM632, SDM636, SDM660, SDM670, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-KAMO- 181120/1855

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-KAMO- 181120/1856
			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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-KAMO- 181120/1857

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

N/A02-Nov-207.27.2Retworking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9206, MDM9607, SA8155P, Sahpan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SX8150, SM8150, SM7150, SX81200Htps://w ww.qualco mm.com/c ompany/p roduct- sapdragon Industrial 107, Snapdragon Industrial 107, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, SA8155P, Sagana, SC7180, SC8180X, SDM845, SDM670, SDM710, SDM845, 	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/AO2-Nov-207.27.2CVE ID : CVE-2020-3684Image: Configuration of 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 Mobile, Snapdragon Mobile, Snapdragon Mobile, 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, SDM670, SDM710, SDM845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55,Image: Image:				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,		
N/A 02-Nov-20 7.2 for the second seco				CVE ID : CVE-2020-3684		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	181120/1858

1194

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-KAMO- 181120/1860

0-1

1-2

2-3

4-5

5-6

7-8

6-7

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, 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		
			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://w ww.qualco mm.com/c	
Improper Input Validation	02-Nov-20	7.8	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 Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-KAMO- 181120/1861

1196

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, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-BITR- 181120/1862

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

			CM02E0 CVD2120		
			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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-BITR- 181120/1864

0-1

1-2

2-3

4-5 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & 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 Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-BITR- 181120/1865
CVSS Scoring Sca	le 0-1	1-2	2-3 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 Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-BITR- 181120/1866
			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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-BITR- 181120/1867

0-1

1-2

2-3

4-5

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 Overfow issue (CVE-2019-16336,CVE- 2019-17519) and Silent Length Overflow issue(CVE- 2019-17518) mentioned in sweyntooth paper)' in Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-BITR- 181120/1868

0-1

1-2

2-3

4-5

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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial 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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-BITR- 181120/1869

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Nobile, 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, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco	H-QUA-BITR- 181120/1871

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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/c ompany/p roduct- security/b ulletins/oc 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	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-BITR- 181120/1872	
CVSS Scoring Sca	le <u>0-1</u>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 1204						

1204

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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-BITR- 181120/1873

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Nobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-BITR- 181120/1874
Improper Validation of	02-Nov-20	10	u'Buffer overflow occurs while processing SIP	https://w ww.qualco	H-QUA-BITR- 181120/1875
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

1206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3654	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
qcs610					
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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1876

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

8-9

Use After Free 02-Nov-20 4.4 Use After Free 02-Nov-20 Use After Free Disting Free Free Disting Free Free Pather Free Disting Free Free Disting Free Free Free Free Free Disting Free Free Free Free Free Free Free Fre	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free02-Nov-204.4u'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 Wearables, Snapdragon Wired Infrastructure and Networking in Agatti,Https://w ww.qualco mm.com/c ompany/p roduct- 181120/1877				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, SDM450, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,		
APQ8053, Bitra, IPQ4019,		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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	• •

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1878
Buffer Copy			u'Remote code execution can	https://w	
without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	10	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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-QCS6- 181120/1879

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1880

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, 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, 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1881

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

			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 C	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 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, SDM670, SDM710, SM8450, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1882
Buffer Copy (without	02-Nov-20	10	u'Possible buffer overflow while updating output buffer	https://w ww.qualco	H-QUA-QCS6- 181120/1883

1212

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/c ompany/p roduct- security/b 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 Overfow 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1884

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, 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 Consumer Electronics Connectivity, Snapdragon Consumer IDT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCS6- 181120/1885

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA81- 181120/1886

0-1

1-2

2-3

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		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	8.3	CVE ID : CVE-2020-11125 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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-SA81- 181120/1888

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	security/b ulletins/oc tober- 2020- bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	CVE ID : CVE-2020-11155 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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA81- 181120/1889

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober-	H-QUA-SA81- 181120/1891

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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 Woice & 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA81- 181120/1892

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Improper Validation of Array Index02-Nov-2010SXR2130 CVE ID : CVE-2020-11173Improper Validation of Array Index02-Nov-2011u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon, Vice & Music, Snapdragon Wearables, Snapdragon, Weather and Infrastructure and Infrastructure and Infrastructure and Infrastructure and Infrastructure and INPQ8098, Bira, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, IPQ8074, Kamorta, IMD99650, UCA9531, QCM2150, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Sajan, SC8180X, SDM620, SDM630, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM630, SDM632, SDM630, SDM630, SDM632, SDM630, SDM630, SDM632, SDM630, SDM630, SDM632, SDM2450, SXR1130, SXR2130 CVE ID : CVE-2020-11174H-QUA-SA81- 181120/1894Improper Validation of02-Nov-2011u'Buffer overflow occurs while processing SIPhttps://w ww.qualco	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Indexu'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9650, MDM9667, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6390, QCA9531, QCM2150, QCA544, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SCB180X, SDM632, SDM636, SDM660, SDM670, SDM429, SDM429V, SDM630, SDM632, SDM632, SDM6450, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-11174H-QUA-SA81- HUA-SA				SXR2130		
Improper Validation of Array Index02-Nov-204.6issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Conpute, Snapdragon Consentivity, Snapdragon Consentivity, Snapdragon Muited Infrastructure and Networking in Agatti, NP0809, APQ8007, APQ8007, MDM9607, MP08098, Bitra, IPQ4019, IPQ5018, IPQ5014, IPQ50148, IPQ8064, ompany/p roduct- ubletionHttps://w H-QUA-SA81- 181120/1893 UIE100Improper Validation of Array Index02-Nov-204.6FH-QUA-SA81- UIE20018, IPQ6018, IPQ8064, OC4953, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, Sumpdragon Vice4 IPQ5018, IPQ8074, Kamorta, MDM9650, MSM89905, SSA8155P, Saipan, SCG180X, SDA60, SDM640, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM670, SDM710, SDM845, SDM20, SXR1130, SXR2130 CVE ID: CVE-2020-11174H-QUA-SA81- UIE200-SM81- UIE200-SM81- UIE200-SM81- UIE200-SM8150, SM8450, SXR1130, SXR2130 CVE ID: CVE-2020-11174				CVE ID : CVE-2020-11173		
U2-Nov-20 10 a Bandr Overnett Oceans intepsty / 1	Validation of	02-Nov-20	4.6	issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wieta Snapdragon Wieta Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, 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	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	-
while processing SIP ww.qualco 101120/1094		02-Nov-20	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
Array Index			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	mm.com/c ompany/p 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA81- 181120/1895
			Snapdragon Wearables in		

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		
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-3673 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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA81- 181120/1896

0-1

1-2

2-3

4-5

5-6

6-7

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA81- 181120/1897
sa515m	I				
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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-SA51- 181120/1898

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 Woice & 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/b ulletins/oc 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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-SA51- 181120/1899

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc	H-QUA-SA51- 181120/1901

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	tober- 2020- bulletin	
Improper Input Validation	02-Nov-20	4.8	CVE ID : CVE-2020-11155 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 Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11156	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-SA51- 181120/1903

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA51- 181120/1904
			Shapuragon wheu		

1227

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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p	H-QUA-SA51- 181120/1906

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & 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, 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	roduct- security/b ulletins/oc tober- 2020- bulletin	
Incorrect Default Permissions	02-Nov-20	4.6	CVE ID : CVE-2020-11174 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

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

N/A02-Nov-204.6Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, BST 20, SWR150, SWR250, SWR210 CVE D1 : CVE-2020-3638bulletinN/A02-Nov-204.6u'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 Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile,	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
 N/A 02-Nov-20 4.6 MENT NC partition from the SMEM TOC contents populated by XBL Loader and applies them without validation' in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Nobile, mm.com/c Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wired N/A 02-Nov-20 4.6 MC Networking in Agatti, Security/b APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, tober- MDM9150, MDM9205, 2020- MDM9150, MDM9205, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA4155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDM670, SDM670, SDM710, SDM845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM630, SDM636, SDM640, SDM670, SDM710, SDM845, SDM630, SDM636, SDM640, SDM670, SDM710, SDM845, SDM630, SDM630, SDM636, SDM640, SDM670, SDM710, SDM845, SDM630, SDM630, SDM636, SDM640, S				Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	bulletin	
	N/A	02-Nov-20	4.6	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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, 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,	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	•

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 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, SDM670, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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(C VE-2019-19193) mentioned in sweyntooth paper)' in Snapdragon Auto,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-SA51- 181120/1910

0-1

1-2

2-3

4-5

5-6

6-7

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, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, QCA6390, QCA6574AU, SOM6125, QCN7605, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020-	H-QUA-MDM9- 181120/1911

0-1

1-2

2-3

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, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM898, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA45, SDM429, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	bulletin	
qca4531					
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,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA4- 181120/1912

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct-	H-QUA-QCA6- 181120/1914
CVSS Scoring Scal	le 0-1	1-2	2-3 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, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM450, SDM630, SDM632, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	security/b ulletins/oc tober- 2020- bulletin	
N/A	02-Nov-20	4.6	CVE ID : CVE-2020-3673 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1915

1235

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 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1916

0-1

1-2

2-3

4-5

5-6

6-7

7-8

3-4

8-9

Improper Input Validation02-Nov-207.8SM8250, SXR1130, SXR2130 CVE ID : CVE-2020-3690H-QUA-QCA6- 101/101/101/101/101/101/101/101/101/10
Improper Input Validation02-Nov-207.8u'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 Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Nired Infrastructure and Networking in Agatti, APQ8005, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA6390, QCS404, QCS405, SDR865, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,H-QUA-QCA6- security/b
Improper Input Validation02-Nov-207.8connection 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 Consumer Electronics Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer Nobile, Snapdragon Consumer Electronics Connectivity, Snapdragon Io1, Snapdragon Muto- Snapdragon Io1, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ809, APQ8017, APQ809, APQ8017, APQ809, APQ8017, APQ809, APQ8017, APQ8050, MDM9670, MDM9640, MDM9607, MDM9640, MDM9670, MDM9640, MDM96

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 Nobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM950, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SM8250, SXR1130, SXR2130 	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1918
Improper	02-Nov-20	4.8	u'Buffer over-read issue in	https://w	H-QUA-QCA6-

0-1

1-2

2-3

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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250 CVE ID : CVE-2020-11141	ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1920
Buffer Copy without	02-Nov-20	8.3	u'Buffer overflow while processing a crafted PDU	https://w ww.qualco	H-QUA-QCA6- 181120/1921

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')	ize of Input Classic uffer		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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55 CVE ID : CVE-2020-11154	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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 Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1922

0-1

1-2

2-3

4-5

5-6

6-7

8-9

7-8

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 Wired Infrastructure and Networking in QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1923
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-20	4.6	CVE ID : CVE-2020-11156 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 Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064,	https://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1924

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

			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	2-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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1925
Integer 02 Overflow or	2-Nov-20	6.4	u'Buffer over-read while processing received L2CAP	https://w ww.qualco	H-QUA-QCA6- 181120/1926

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Wired Infrastructure and Networking in APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	
			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 Woice & Music, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1927

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 2020- bulletin	H-QUA-QCA6- 181120/1928

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

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 Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, 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://w ww.qualco mm.com/c ompany/p roduct- security/b ulletins/oc tober- 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

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	I			L	
Out-of- bounds Write			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	out-of- ounds 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			I		
Out-of-	08-Nov-20	4.6	An issue was discovered on	N/A	H-SAM-EXYN-

0-1

1-2

2-3

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	I			I	
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	